Performance Characterization of Hybrid Wireless Network with WiFi Access and WiMAX Backhaul Links for Rural Broadband Applications

A thesis submitted in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

by

Punit Rathod
(Roll No. 04429001)

Under the guidance of
Prof Abhay Karandikar
and
Prof Anirudha Sahoo

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY–BOMBAY
2014

To my parents.

Thesis Approval

The thesis entitled

Performance Characterization of Hybrid Wireless Network with WiFi Access and WiMAX Backhaul Links for Rural Broadband Applications

by

Punit Rathod
(Roll No. 04429001)

is approved for the degree of

Doctor of Philosophy

Examiner	Examiner
Guide	Co Guide

Chairman

Date: _____

Place: _____

Declaraton

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.
I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Date: Punit Rathod

Abstract

Wireless communication is a key ingredient in bridging the digital divide by overcoming a lot of limitation factors of the wired networks; viz. a) right of way for laying cables, b) cost of installing and maintaining the fixed wired infrastructure and c) low return on investment. As wireless networks provide both technical and practical advantages over wired networks in bridging the digital divide and enabling reach of networks to a wider spectrum of people, this thesis specifically looks at one particular method of deployment of wireless networks.

We consider a wireless network where individual client nodes use a low-cost and widely popular wireless radios from the IEEE 802.11 family (also popularly known as WiFi). This gives many advantages that include affordability, availability, variety and simplicity of end user devices. In order to ensure connectivity of the last mile IEEE 802.11 based access network, we consider a fixed wireless infrastructure network based on IEEE 802.16 (also popularly known as WiMAX).

One of the main reasons for considering a wireless network is improving the tele-density of rural subscribers that lag behind the urban subscribers by a ratio of almost 1:2 in the favor of urban subscribers as per the Telecom Regulatory Authority of India (TRAI) statistics from March 2013. In order to understand the network deployment in a better manner, the performance of the networks that involve two different medium access control technologies in the access and the backhaul need to understood.

There are multiple methods to study and understand the performance of large wireless networks. Setting up a pilot network and understanding the performance of the network using measurements from the live network is one of the methods. This method may give the most accurate results, however is not scalable as there may be many different conditions and scenarios of deployment to be considered; viz. different arrival rates at client nodes, different location of client devices, different number of client devices connected to the access network. An alternative method to study the performance is using simulation of networks using open source and

commercial network simulators like NS2, NS3, QualNet, Opnet and Glomosim. The simulation method, solves the problem of varying the different conditions to be measured very effectively. Many different simulation topologies can be configured and statistics can be measured by the simulation tool to evaluate the performance of the networks. In simulations, the real world time is the amount of time for which we want to evaluate a particular network and the simulation time represents the amount of time taken to simulate the network. In simple network topologies, the simulation time is less than the real world time, making simulations effective in terms of time. However, with complex topologies and in heavy load conditions where statistics have to be gathered for every packet that is generated in the simulation, the simulation time quickly becomes larger than the real world time. Hence, the effectiveness of the simulation method is only limited by the amount of compute resources available. Simulations also loose some level of detail from the actual measurements from a live network. The third alternative to understanding the performance of a network is to model the performance of the network analytically. This method involves making certain simplifying assumptions on the network to make the network model analytically tractable, but provides significant advantages in terms of quickly providing results for the performance of networks.

In this thesis, we address the problem of understanding the performance of a hybrid network analytically in two parts. We first determine the time taken between two packet departures from an IEEE 802.11 network by modeling the medium access control of the IEEE 802.11 network. And later we use a queuing network theory to model the backhaul network with IEEE 802.16 based scheduler to determine the waiting time of packets before departing the nodes. This enables us to understand the behavior of different building blocks of the network and how they influence the traffic.

This thesis also uses all the three tools for evaluating the performance of a network for different purposes. Analytical modeling is used to determine performance metrics in the network. Simulation results are used to validate the analytical model. And a test-bed is used to verify if the model is able to predict the performance of the network within acceptable limits. We determine that the analytical model for IEEE 802.11 and IEEE 802.16 based networks matches very well with the simulation results from QualNet network simulator. From the testbed results for an IEEE 802.11 network, it is also determined that the analytical model follows the same trend in values for collision probability and packet attempts.

While studying the deployment of both IEEE 802.11 and IEEE 802.16 networks, we also

study the coexistence of different types of client devices within a close vicinity. This study concentrates on the deployment in urban areas where both IEEE 802.11, Local Area Network (LAN), and IEEE 802.16, Wide Area Network (WAN), will coexist with a small geographical area. Existing measurements in literature show that the LAN and WAN devices that are within proximity of each other may cause interference to each other even if they are operating on non-overlapping channels. This is due to out-of-band emissions that exist in both the LAN and WAN devices. In order to address the coexistence of devices, we propose schemes to mitigate the interference by arbitration of wireless channel resources in time domain. Using testbed measurements, we show that the impact of using packet protection schemes proposed by us on the performance of the IEEE 802.11 wireless LAN is minimal.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Communication has always been an integral part of the society. With advances in technology, communication has become more and more accessible. From shared Internet access machines to hand-held devices, the access to information and ability to communicate easily with others has helped in rapid growth of society, both in the urban and rural setup. Network penetration is being viewed as one of the key indicators of the development of a nation. Specifically, broadband penetration is essential to enable and provide a variety of services to the masses. A significant proportion of government supported services are becoming increasingly dependent on access to network connectivity. In addition to enabling services like Unique Identification (UID) [1] and secure mobile payment authentication, providing access to information is also of significant importance.

In a country like India, with a population of 1.2 billion as of 2011 census and growing [2], there is a huge disparity in the quality of Internet access across the urban and rural population. As on March 2013, India boasts of a wired-wireless combined telecom subscriber base of 900 million, resulting in a tele-density of more than 73% [3]. Even with these promising numbers, it is important to note that 61% of the subscribers are from Urban areas and only 39% from Rural areas [3]. Comparing this with the population distribution according to the census of the country, the Urban areas constitute for a paltry 37% of the entire population [2]. Hence, less than 40% of the population accounts for more than 60% of the telecom subscribers of the country. Within this, even with a very conservative definition of broadband of 256 kbps and above, the broadband subscribers contribute to less than 15% of all the subscribers. All these factors point to a very wide digital-divide in a country like India.

From the above data, it is clear that network connectivity in rural areas is very sparse and

there is a large disparity in the penetration of telecommunications in rural areas as compared to the urban areas. It is very cost-prohibitive for service providers to facilitate good quality wired network connectivity to rural areas [4]. Some of the major bottlenecks in providing quality wired service is getting right-of-way, low return-on-investment (RoI), unreliable power supply, and high capital expenses [5, 6]. However, in the parallel market of television penetration, satellite TV has seen a rapid rise in India [7]. One of the primary reasons for this rapid growth of satellite based TV distribution is an ability to bypass the requirement of laying cables to homes. Hence, wireless networks become a very important technology in providing connectivity to the rural population. Further evidence is provided by the growth rate of wireless subscribers in every quarter in India as seen in Figure 1.1.

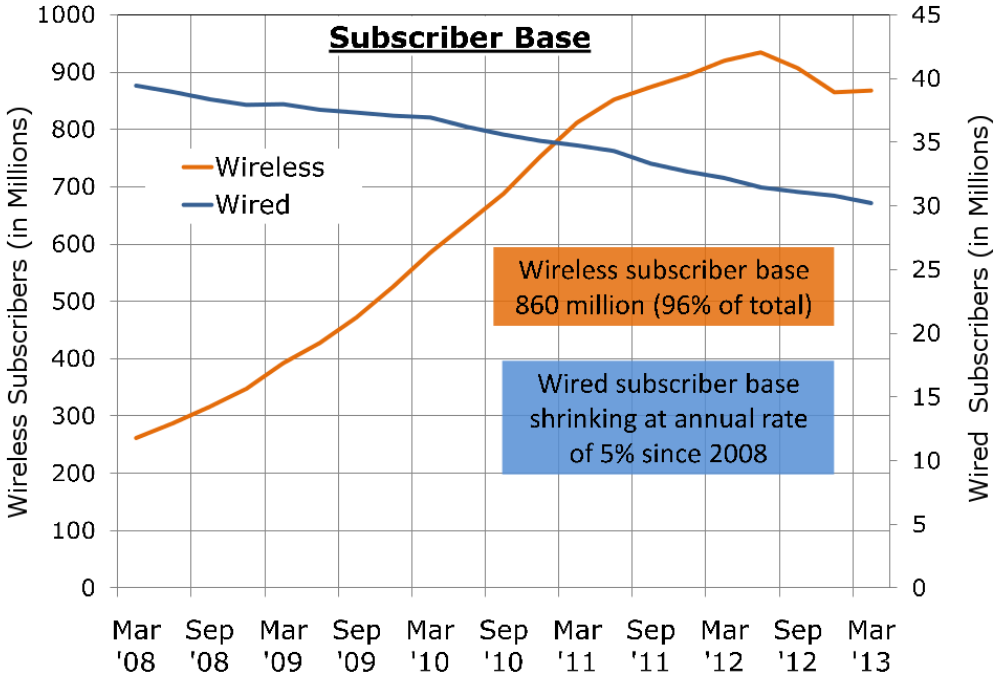


Figure 1.1: Growth of Wireless Subscribers in India

In this thesis, we concentrate on one of the possible wireless network topologies to bridge the digital divide. We discuss various building blocks involved in the network topology and determine the performance characteristics desired in such networks to help in the deployment.

1.1 Bridging the Digital Divide

The habitation of people in the urban and rural areas is very clustered [8]. Figure 1.2 shows the distribution of the population share in India. In the figure, a habitat is denoted by the number of households in a single cluster, the vertical axis denotes the number of such habitat clusters and the size of the bubble denotes the percentage share of population that resides in the particular habitat cluster. The horizontal axis denotes the size range of the individual habitats in terms of number of households.

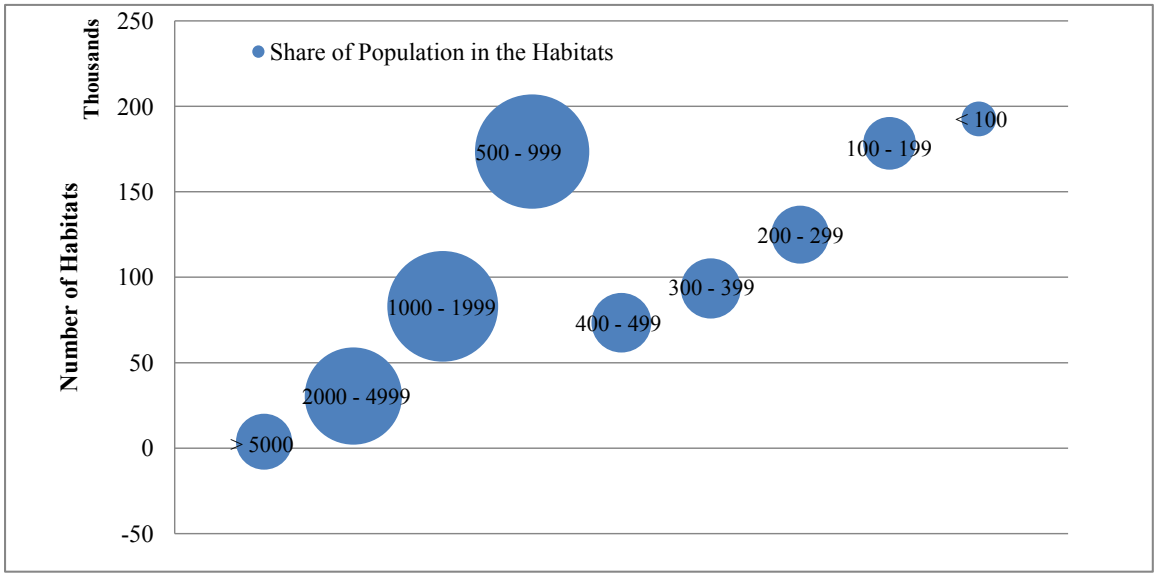


Figure 1.2: Population distribution across different habitat clusters in terms of the habitat size

It is evident that urban areas, denoted by clusters of more than 5000 households, are very densely populated; but still represent a minority of the population. A significant share of the population is in clusters of average density between 1000 and 5000 households; representing mid-sized towns. Finally, rural areas which are sparsely populated, with smaller sized clusters of less than 1000 households, represent a very small fraction of the total population. The clusters of households representing the rural areas are small in size, but are spread across a few hundred thousands locations. This distribution of population in conjunction with poor rural tele-density makes the problem of bridging the digital divide hard. The main challenge is to provide network connectivity to the smaller clusters of less than 1000 households while keeping costs reasonable for both the end user and the operator in order to maintain sustainability. Wireless networks provide a viable alternative to bridge the digital divide and enable communication to a larger percentage of the population at reasonable cost [9, 10]. We propose an architecutre to achieve

this objective using wireless networks.

Consider a network topology as shown in Figure 1.3. The network is built using a hierarchical architecture. Connectivity to a cluster of users is provided using low-cost IEEE[1] 802.11 [11], also called as WiFi [2], devices. The cluster of users served by the local wireless network is aggregated at a central node also referred to as an Access Point (AP) in IEEE 802.11. The AP serves as a gateway node for the cluster of users and is connected to the Internet using a dedicated network connection.

In order to remain cost-effective, the network connection to the aggregating gateway node is also provided using a dedicated wireless link. This dedicated wireless link is responsible for replacing a wired network connectivity to the cluster of users and cover larger distances. The dedicated network connectivity can be realized using wireless by one of the following options, (a) point-to-point IEEE 802.11 links with directional antennas to cover large distances or (b) IEEE 802.16 [12], also called as WiMAX [3] links.

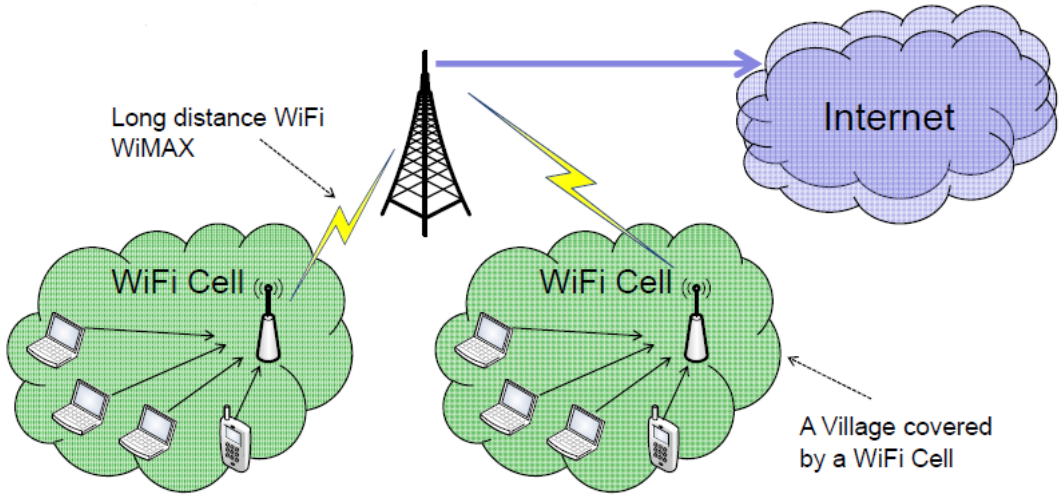


Figure 1.3: Hybrid Network Topology

As seen in Figure 1.3, the local wireless network is providing network access to the users as a last mile connectivity. This is referred to as the *Access Network* in the rest of the thesis.

[1] Institute of Electrical and Electronics Engineers

[2] The IEEE 802.11 standard refers to the Wireless Local Area Network (WLAN) also referred to as Wireless Fidelity (WiFi). In this thesis, we use the terms IEEE 802.11, WiFi and WLAN interchangeably to refer to IEEE 802.11 based protocols.

[3] The IEEE 802.16 standard refers to the Worldwide Interoperability for Microwave Access (WiMAX). In this thesis, we use the terms IEEE 802.16 and WiMAX interchangeably to refer to IEEE 802.16 protocols.

The aggregated connection at the Access Point (AP) of the access network is connected to the Internet using a network referred to as the *Backhaul Network* in the rest of the thesis.

The access network rides on the popularity of IEEE 802.11 standard and the easy availability of low-cost devices. This provides the flexibility in keeping the cost of deploying the network low. We also refer to these individual IEEE 802.11 networks with the access point along with the corresponding client nodes connected to the access point as a *cell*.

The backhaul network uses long-distance IEEE 802.11 links or IEEE 802.16 network for connectivity. Each end point of the backhaul network enables connectivity to one or more IEEE 802.11 cells (or access networks). These individual cells may be spread out over a range of few kilometers. The backhaul network end point is connected to the rest of the backhaul network using a long-distance IEEE 802.11 link or other wireless technologies like IEEE 802.16.

This basic architecture has several key benefits:

- Access network devices can exploit availability of low-cost IEEE 802.11 devices.
- The backhaul network can be independent of the technology used in the access network.
- Coverage required would be clustered around villages and individual IEEE 802.11 cells will not require a lot of radio resource planning.
- Clustered and spread out IEEE 802.11 cells enable simple algorithms in the backhaul network for scheduling.

A network deployment using such a topology would require effective a-priori capacity planning to ensure that the network is capable of handling the load generated in the network. An ad-hoc network deployment with haphazard installation of IEEE 802.11 cells and backhaul network elements can easily result in excess provision in low-load areas or under provisioning in heavy load areas.

In order to analyze the performance of the proposed network, we need to determine how the network elements behave under different load conditions, impact on the queue length build up at the backhaul network and the increase in delays at aggregating nodes (access points). Both the access network (IEEE 802.11 cell) and the backhaul network operate on different technologies and different deployment considerations. They may have different congestion control and scheduling algorithms. This makes the analysis of the entire hierarchical network as a single entity very complex. One of possible methods is to model the entire topology as a

queuing network with each IEEE 802.11 access point and the IEEE 802.16 base station is to be treated as a queue as shown in Figure 1.4

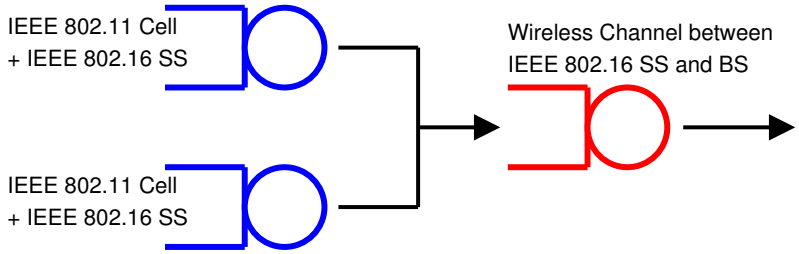


Figure 1.4: Hybrid Network Topology represented using a Queuing Network

1.2 Main Challenges

The main challenges involved in the study of the hybrid network are as follows:

- Determine the factors and metrics that impact the performance in a hybrid network topology with different technologies in the access network and the backhaul network.
- Is it possible to determine the behavior of individual network elements in a hybrid network independently?
- When using different technologies in the hybrid network topology, do they coexist gracefully?

In order to simplify the study of such a hybrid network topology, we look at each queue in the network independently. The access network consists of an IEEE 802.11 access point with a group of client nodes connected to it. The backhaul network connects one or more access points to a central base station which in turn acts as a gateway to the Internet.

1.2.1 Access Network

The existing results available in the analysis of IEEE 802.11 networks [13–21] mainly concentrate on modeling the wireless contention in saturated and non-saturated conditions. In addition to that, majority of the results provide average times between two consecutive successful packet transmissions from an IEEE 802.11 network. This solves only a part of the problem to model

the overall hybrid network with a queuing network where it is essential to have a better understanding of the departure process of the IEEE 802.11 cell.

The significance of this departure process model of IEEE 802.11 cell lies in its ability to use the departure as an independent arrival process in a complex network topology. This allows analysis of a complex network topology without having to model the details of the Medium Access Control (MAC) of individual IEEE 802.11 cells.

In this thesis, we extend the work done by the authors in [14], for the non-saturation case using a fixed point method. We introduce the model for queue length in the fixed point model and determine the collision probability, attempt rate and queue status. With these probabilities, we use random sums in probability to determine the distribution of time between two successful packet transmissions in an IEEE 802.11 network cell.

Most of the existing results in literature concentrate on identical arrival rates at each node in the IEEE 802.11 cell. In this thesis, we generalize the non-saturation fixed point model to incorporate different arrival rates at each client node. We model only the MAC layer of the protocol and do not go into issues related to the Physical Layer to retain analytical tractability.

1.2.2 Backhaul Network

The backhaul network analysis is very typical to the choice of topology considered by us. We also have a specific assumption in the network description where the arrivals to the backhaul network are generated according to the departures from the IEEE 802.11 cells. Depending on the nature of deployment considered, individual IEEE 802.11 cells are likely to be geographically distant.

With these assumptions, we model the IEEE 802.16 based backhaul network using a GI/D/1 queue. Average waiting time and utilization of the backhaul network base station are determined for varying number of IEEE 802.11 cells connected and various loads at each IEEE 802.11 cell. In this thesis, we limit ourselves to the analysis of identical loads at each IEEE 802.11 cell connected to the IEEE 802.16 base station.

1.2.3 Coexistence of Competing Technologies

In the network topology discussed in Figure 1.3, the IEEE 802.11 access network and the IEEE 802.16 backhaul network operate on different technologies but the infrastructure devices are

collocated. However, from the device perspective, the radio interfaces of IEEE 802.11 and IEEE 802.16 are separate. It has been observed that these competing technologies do not coexist very well with each other [22].

Several authors have studied coexistence of IEEE 802.11 and IEEE 802.16 in same channel scenarios and collocated radio interfaces [22–27]. In case the radio interfaces of IEEE 802.11 and IEEE 802.16 are collocated on the same platform, signaling is possible across the interfaces to avoid interference.

However, in the topology under consideration, the client devices, with IEEE 802.11 radio interface, may interfere with the subscriber station with IEEE 802.16 radio interface. Both these radio interfaces are not collocated on the same platform. This makes coordination across these devices challenging. In this thesis, we propose schemes to mitigate the interference across non-collocated radios on adjacent channels.

1.3 Main Contributions of the Thesis

The main contribusions of the thesis are as follows:

1. **Analysis of IEEE 802.11 based network in Non-Saturation condition with homogeneous arrivals across client nodes**. We use the fixed point method to determine collision probability, attempt rate and queue status. Using these, we determine closed form expressions for the time between two successive packet departures from an IEEE 802.11 cell (the exit process). In the homogeneous case, each client device associated with the access point is assumed to have identical arrival process. We validate the results from the analytical model using QualNet simulations.

2. **Extension of the Non-Saturation IEEE 802.11 analysis for non-homogeneous case where client nodes connected to the access point have different arrival rates**. A multi-variate fixed point method is used to determine collision, attempt and queue status probabilities for nodes in the network. We also determine the mean departure time and the variance in the departure times for this condition. We validate the analytical model using QualNet simulations.

3. **Setting up an Experimental testbed for validating the Non-Saturation IEEE 802.11 homogeneous and non-homogeneous analytical models**. We collect statistics from the

wireless drivers for various metrics like collisions, inter packet times and waiting times to verify the analytical model. In order to achieve accurate results, modifications are made to the wireless drivers to enable the logging of statistics across different nodes in a time synchronized manner. The results obtained from the analytical model are found to follow the trends observed in testbed results.

4. **Analysis of a hybrid IEEE 802.16, IEEE 802.11 network based on Time Division Multiple Access (TDMA) scheduling on the uplink**. The backhaul network with TDMA scheduling is modeled as a GI/D/1 queue. The arrivals to the GI/D/1 queue are generated using the exit process derived in IEEE 802.11 exit process. We determine performance indicators for queue length and waiting times at the backhaul network for safe operation regions. We validate the analytical model using QualNet simulations.

5. **Studying the issues of coexistence of non-collocated IEEE 802.11 and IEEE 802.16 networks while operating in adjacent channels**. We have proposed solutions to mitigate the coexistence issues enabling both IEEE 802.11 and IEEE 802.16 networks to operate simultaneously in close proximity. A simple solution based on Clear to Send (CTS) message with power-control is proposed in a dual-radio (IEEE 802.11 and IEEE 802.16) node to disable transmissions from an interfering IEEE 802.11 device. We have implemented the proposed scheme on IEEE 802.11 testbed to verify the effectiveness of the scheme.

1.4 Organization of the Thesis

In Chapter 2, we discuss the existing literature and the state of the art in the performance study of wireless networks. We discuss the results related to testbed measurements, simulations and analytical modeling of IEEE 802.11 networks. We also discuss the main results in IEEE 802.16 network analysis. Finally, we discuss the results in coexistence studies of collocated and non-collocated wireless networks in same channel and adjacent channels.

In Chapter 3, we describe the formal problem formulation and present a preliminary analysis of IEEE 802.11 network in saturation condition. This analysis provides an elementary understanding of the IEEE 802.11 network performance.

In Chapter 4, we discuss the analysis of IEEE 802.11 based networks. We discuss both

cases of homogeneous and non-homogeneous arrivals at each node in the access network in this chapter. In the case of homogeneous arrivals, we determine a closed form expressions for the departure process from a cell (time between two successive packet transmissions). In the case of non-homogeneous arrivals, we determine average and variance for the departure process. A validation of the analysis using simulations is also discussed in this chapter.

In Chapter 5, we discuss the main issues involved in setting up an indoor IEEE 802.11 testbed in the lab for the purpose of validating the analysis of an IEEE 802.11 network. In this chapter, we discuss the hardware choice, software tools used, and driver modifications for the purpose of performing measurements. We also discuss the similarity in trends observed in the testbed results and analytical model in this chapter.

In Chapter 6, we discuss the analytical model for IEEE 802.16, IEEE 802.11 based hybrid network. A GI/D/1 model of the backhaul network is discussed with arrivals based on an IEEE 802.11 access network. Validation of the model using simulations is also discussed in this chapter.

In Chapter 7, the issues with coexistence of IEEE 802.11 and IEEE 802.16 networks are discussed. Schemes are proposed to protect IEEE 802.11 transmissions and IEEE 802.16 transmissions. Implementation details of IEEE 802.16 transmission protection in the indoor testbed are discussed in this chapter.

In Chapter 8, we present the concluding remarks and directions for future research.

Chapter 2

Overview of Main Results in Literature

In this chapter, we discuss the existing literature in the domain of IEEE 802.11 Analysis and Coexistence. A brief overview of the IEEE 802.11 standard, the associated timing parameters, packet formats, protocol functions and configurable parameters are provided in Appendix A.

2.1 Performance Analysis of IEEE 802.11

The analysis of IEEE 802.11 Wireless Local Area Networks (WLAN) is well-known to be a tough problem due to the interaction of different queues via the feedback from the AP. The analytical modeling of IEEE 802.11 can be broadly classified into saturated case and non-saturated case analysis. For the saturated case, a popular and accurate analytical approach is the fixed-point analysis based on the independence assumption (also called the decoupling approximation). The independence assumption originates in the work of Bianchi [13] and it states that in steady state, the attempt processes of various nodes are independent. Subsequently, its applicability has been extended by several authors (see for example [14], [28], etc.) and it has been proven to be accurate for large number of nodes (n) in [29].

While the saturated case leads to relationships between the collision and attempt probabilities, in our case we also get additional relationships with the probability of the queue at a node being empty. The three way relationship can be solved numerically to obtain the desired quantities in steady state. In [15], it is suggested that for analyzing downlink Transmission Control Protocol (TCP) throughput, the saturation case results can be used with the number of nodes (n) replaced by suitable effective n'.

2.1.1 Saturated Case Analysis of IEEE 802.11 MAC

Based on the probabilities of collision, attempt, and empty queue, the distribution of the inter-exit times can be derived. The inter-exit time has also been referred to as service time by several researchers. The mean service time for saturation case has been derived in [16–18]. The service time distribution has been derived for the saturation case in [30–32] and for near-saturation case in [33].

Authors in [16] use a Discrete Time Markov Chain (DTMC) as used in [13] with extensions for finite number of retransmissions of the wireless nodes. The packet drop probability is determined after a specific number of retransmissions have happened in the network. Using the packet drop probability and the average amount of time taken between two packet drops, the authors also determine the average values for time between two successful packet transmissions in the network.

The IEEE 802.11 protocol analysis in the saturation in the presence of hidden nodes is performed in [34]. The DTMC model is used with extensions provided for capturing the state of nodes in the presence of interference from hidden node transmissions. The authors also provide a novel approach to model the network state using a Markov chain. In this new model the authors use the state of the Markov chain to represent the entire network instead of a single node as done in [13]. This approach greatly improves the accuracy of the model in the saturation condition in presence of hidden node terminals.

The performance of a IEEE 802.11 based network in the presence of fading channels is also modeled in [35]. Authors in [36] also present a model for both the IEEE 802.11 Distributed Coordination Function (DCF) and basic mode of channel access in the presence of Rayleigh Fading channels and adaptive rate fall-back mechanism.

2.1.2 Non-Saturated Case Analysis of IEEE 802.11 MAC

For the non-saturated case, the mean service time is derived in [19] and [20]. In [21], the authors empirically compare the observed service time distribution with several known distributions and show that exponential distribution provides a good approximation to the service time.

A M/M/GI/K based queuing model is used in [19] to determine the probability that there are k packets in the queue at a given time. From the number of packets in queue and the channel access time computed from the DTMC the average delays for packets is determined.

Authors in [20] use a similar approach with embedded Markov chain and a DTMC for the queue status with transition probabilities determined using the attempt rate in the IEEE 802.11 network and the arrival rate of new packets in the queue. The authors determine bounds for the throughput for TCP performance in a nonsaturated IEEE 802.11 network.

Several researchers have derived the probability generating function (PGF) for the service time in non-saturated case [37] [38] [39]. The probability density function (PDF) can be numerically computed from the PGF and a closed form for the PDF is not available to the best of our knowledge.

A network with mixed traffic from saturated and nonsaturated sources is has also been evaluated in [40]. The authors model the network using a fixed point model to determine probabilities for collision and attempt. A queue model is used for Poisson arrivals at individual nodes. The mean channel access time is estimated and compared with simulation results. The distribution of the queue length is also computed to determine the average waiting time for packets in the network.

Authors in [41] also determine the performance of an IEEE 802.11 network in the presence of fading channels and capture condition. A 3-dimensional Markov chain based on the DTMC by [13] is used to model the performance of the network. The authors also determine the probability of call block in cases where specifi Quality of Service (QoS) is required like Voice over IP (VoIP). Average queue length in presence of different traffic loads is also determined.

2.1.3 Open Problems and Our Contributions

We derive a closed form approximation for the PDF of the inter-exit time for packets, whose parameters are obtained by fixed-point analysis. We define inter-exit time as the time observed by an external observer between two successful packet transmissions in the network. This is different from the service time of a node. Despite a plethora of literature related to IEEE 802.11 WLANs, to the best of our knowledge, a closed form expression for the probability distribution function, has not been derived. Moreover, our methodology of extending the fixed point analysis to the non-saturated case is novel. This methodology can help us in extending this framework to multi-hop and mesh networking scenarios.

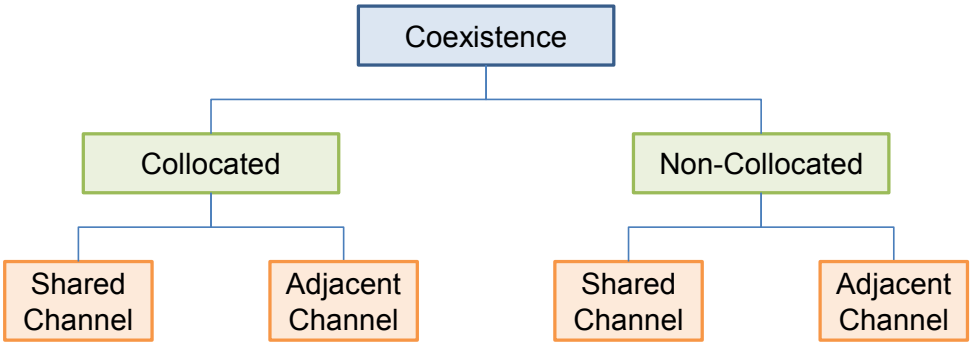


Figure 2.1: Classification of Coexistence Mitigation Schemes

2.2 Coexistence of Wireless

In a given geographical area, multiple wireless devices operating on different technologies exist. The wireless devices may interfere with each other causing the performance of the wireless networks to degrade. In this section, we look at recent results in mitigation and management of the interference due to coexistence of wireless networks. The related literature can be broadly classified into two categories, collocated and non-collocated coexistence as shows in Figure 2.1.

The wireless devices operating on different technologies may share the wireless channel (same frequency of operation), e.g., WiFi [11] and Bluetooth [42] both operating in the 2402 MHz to 2480 MHz frequency band.

The literature can be broadly classified into collocated coexistence and non-collocated coexistence mitigation schemes. The problem of collocated coexistence across technologies on a multi-radio platform has been studied in [22] [23] and the references therein. Collocation coexistence mainly deals with the coordination across interfaces in a multi-radio platform with a coordination block. The radio interfaces on the multi-radio platform exchange signals through the coordination block to schedule transmissions (either shared channel or adjacent channel).

In the case of non-collocated coexistence, there is further division on the basis of handling shared channel and adjacent channel interference. Non-collocated coexistence across different devices on separate technologies but on the same channel has been studied in [24] [25] [26]. In [24], the authors discuss the impact of non-collocated coexistence when both IEEE 802.11 and IEEE 802.16 devices operate in the same channel. Schemes to mitigate the impact of non-collocated coexistence while operating in the same channel are discussed in [25] and [26].

Non-collocated coexistence of WiFi and Bluetooth falls in the category of both shared channel and adjacent channel coexistence of non-collocated coexistence. This problem has

been well studied in the literature. Authors in [27] and the references therein propose methods to mitigate interference across WiFi and Bluetooth devices when they operate, on the same or adjacent channels, within the 2.4GHz Band.

To the best of our knowledge, the issue of non-collocated coexistence, where, the devices operate on adjacent channels has not received much attention. The focus of this thesis is to discuss the impact of interference due to adjacent channel interference and propose schemes to mitigate the same.

2.2.1 The Problem

The problem of coexistence between WiFi and WiMAX is made severe due to the relaxed transmit spectrum masks [4] mandated by the IEEE standards in the case of WiFi. WiFi networks, by means of design, have been not very efficient in the filters because they were to operate in the license exempt Industry, Science and Medicine (ISM) bands. However, with adjacent bands being used for Fourth Generation (4G) technologies like WiMAX and Long Term Evolution (LTE) [5], the low-cost filter design of WiFi becomes a problem. The problem of coexistence is made more severe due to the channel assignment for 4G technologies.

Consider the transmit spectrum masks as per the IEEE 802.11 [11] and IEEE 802.16 standards [12]. Figure 2.2 shows the transmit spectrum mask for both WiFi and WiMAX devices in the 60 MHz range from the center frequency of transmission of WiFi and WiMAX signal. A typical WiFi/WiMAX signal will occupy 20 MHz of bandwidth. As seen in the figure, beyond the +10 MHz and -10 MHz range, the relative signal strength drops significantly. It can also be seen that the specifications for WiMAX are more stringent as compared to WiFi for out of band transmissions. Even at a separation of -30 MHz (20 MHz away from the transmitted signal), WiFi signal can be legally 10 dB higher than the WiMAX signal.

The difference in transmit spectrum masks becomes significant when we consider adjacent channel transmissions. Figure 2.3 shows the transmission of signals in adjacent channels. The figure represents the WiFi signal in Channel 1 (2412 MHz) and the WiMAX signal in channel

[4]Transmit Spectrum Mask: A transmit spectrum mask quantifies the amount of radio emission allowed by the wireless standard in the frequencies that are outside the intended wireless transmission. The purpose is to define the amount of out-of-band transmission allowed in the adjacent frequency channels

[5]In this thesis, we use the term LTE to broadly refer to the standards in Release 8 and later within the Third Generation Partnership Project (3GPP)

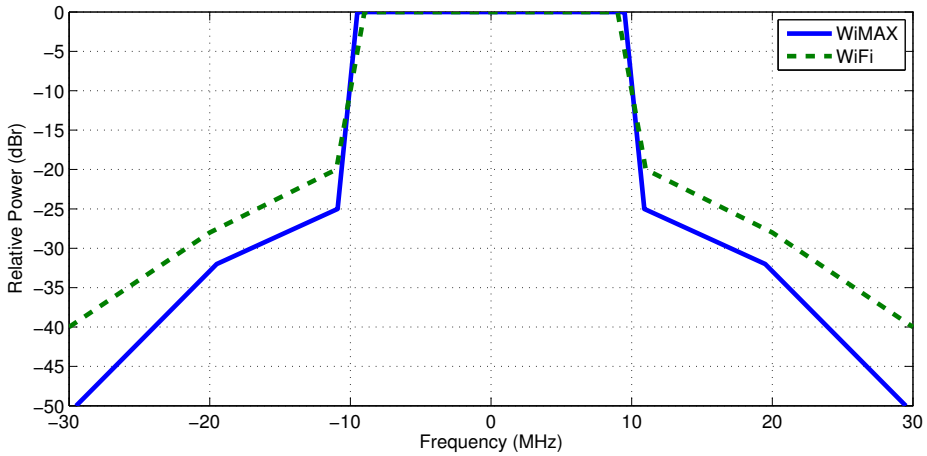


Figure 2.2: Comparison of Transmit Spectrum Mask for WiFi and WiMAX.

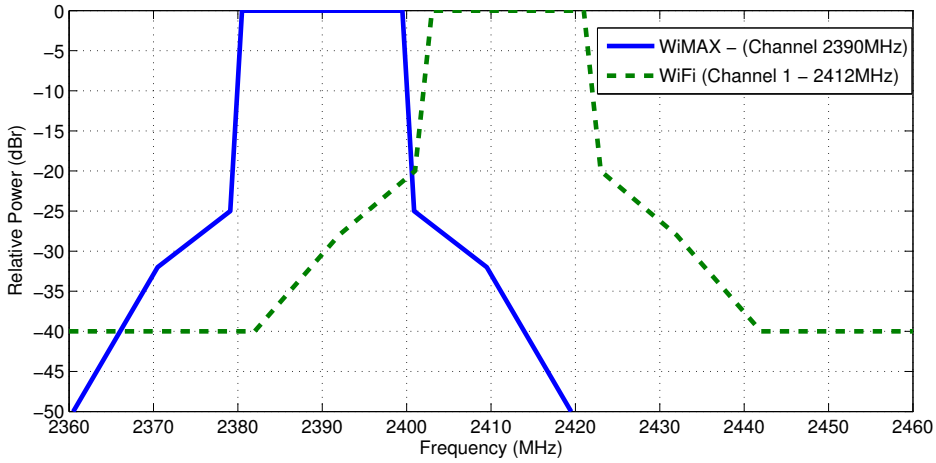


Figure 2.3: Comparison of Transmit Spectrum Mask for WiFi and WiMAX in Adjacent Channels.

with center frequency at 2390 MHz. It can be easily seen that in both the cases, the out of band transmission allows for a significant amount of interference.

2.2.2 Open Problems and Our Contributions

We determine the severity of interference caused by adjacent channel interference due to coexistence of WiFi and WiMAX devices. Based on the study from the literature and experimental measurement, it is established that out-of-band emissions from WiFi and WiMAX have potential to cause interference to each other even while operating in non-overlapping adjacent bands. A time domain multiplexing is desired across different WiFi and WiMAX devices to ensure interference free operation. We propose schemes to mitigate the interference in a network us-

ing coordination across devices. We also setup a testbed to demonstrate the efficacy of the schemes proposed by us and present results to demonstrate that there is very limited impact on the throughput of the WiFi network due to coordination function.

Chapter 3

Initial Analysis of an IEEE 802.11 Cell

In this chapter, we introduce the system model considered in the thesis with the help of a simple IEEE 802.11 network. Initially, we discuss a naïve approach for the analysis of IEEE 802.11 network in Section 3.1. We determine average time between two successful departures using the order statistics. While studying the behavior of the IEEE 802.11 network, we ignore the effect of interference from possible neighboring IEEE 802.11 networks because of the rural context highlighted in Section 1.2.1. As a result of the rural nature of deployment of the networks, we assume little to no interference from other IEEE 802.11 networks. In addition to that, we also consider the IEEE 802.11 network to be deployed in locations like libraries, gram panchayats and town halls, resulting in the entire spectrum of load conditions from low to high within the IEEE 802.11 cell.

Indoor wireless local area networks (WLANs) based on IEEE 802.11 family of standards are by now ubiquitous. As discussed in Chapter 1 and 2, there are two design philosophies catering to different applications; a) An ad hoc networks based on IEEE 802.11 radios for various applications like community networks [43], rescue and defense applications [44], and b) Hybrid networks where 802.11 cells are linked by a backbone mesh network comprising of potentially other technologies such as IEEE 802.16 (see [45] [46] and the references therein).

In the context of this thesis, we use the term hybrid network to refer to networks with different technologies in the access and the backhaul. As discussed in Section 1.2.1 and 1.2.2, we focus on an IEEE 802.11 based access network which cater to the end users, and the aggregated traffic from the access network being catered to by an IEEE 802.16 based backhaul network.

While the interplay between coverage, user capacity, and throughput has recently been understood analytically for isolated 802.11 cells [28], for ad hoc as well as hybrid networks,

as yet there is incomplete understanding of these issues. Engineering such networks is indeed an art and due to the lack of analytical tractability, detailed simulations are often the main tool. This is evidenced by the popularity of simulation tools such as NS2 [47], OPNET [48] and QualNet [49]. The simulation of such complex networks can often be significantly sped up by resorting to analytical approximations for sub-components, whenever such good approximations are available. Towards this goal, we model the exit traffic from an IEEE 802.11 network.

3.1 A Naïve Approach to the Analysis of IEEE 802.11 Wireless Network

In this section, we analyze the performance of a single-hop IEEE 802.11 based wireless network to determine the time taken by a node to successfully transmit a head-of-line (HOL) packet. We model the single-hop network as a server and the contending nodes as arrivals to the server. We determine the service time of the single-hop network depending on the number of nodes contending for channel access. The service time of the single-hop network gives us the overall time taken by any HOL packet (at one of the contending nodes) to be successfully transmitted in the network. Once the service time for the network is determined, the service time for individual nodes can be computed. The analysis is verified using simulations in QualNet, and we observe that the analysis closely matches with the simulation results.

3.1.1 System Model

We analyze the performance of a peer-to-peer IEEE 802.11 based wireless network in a single-hop setting. We consider an infrastructure-less network, where all communication between nodes is direct, without going through an Access Point. To perform the analysis, we define a *cell* as an area under consideration, where nodes contained within the cell can communicate with each other directly in single hop. Consider N nodes in a cell and each node uses IEEE 802.11 based Medium Access Control (MAC) for channel access. Because of the IEEE 802.11 MAC layer, only one transmission can occur at a time in the cell. Viewing the cell as a queuing system, the time between two successful transmissions in a cell can be modeled as the service time of the queue. The underlying MAC layer then becomes the server and the contending nodes, and collisions determine the service times. The arrivals into the queue are the aggregate

arrivals due to all the nodes in the cell. The number of backlogged nodes determines the number of contending nodes in the cell, which affects the service time. We assume a saturation case, where the number of backlogged nodes always remains a constant, i.e., all nodes have at least one packet to transmit at all times. Then the analysis of the service times becomes similar to the analysis of N saturated flows. The system described above is depicted in Figure 3.1.

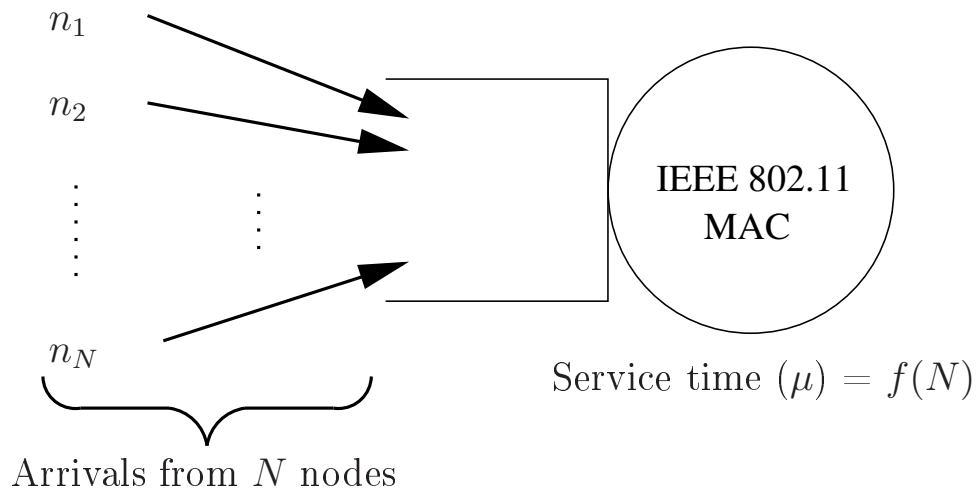


Figure 3.1: Model of a Single Cell Wireless Network with the MAC as Server

We consider the Basic Access mechanism of IEEE 802.11 [6], and all the data packets to be of same fixed length. The Basic Access mechanism of IEEE 802.11 uses only the DATA and Acknowledgement (ACK) packets. The parameters and notations used in the modeling of the system are listed in Table 3.1.

3.1.2 Analysis of Servive Time in a Single-Cell IEEE 802.11 MAC

In Table 3.1, various parameters used in the analysis are listed. Let us consider N continuously backlogged nodes in a network. As the basic mode of access is used, i.e., DATA-ACK, the time consumed in transmission of the packets (excluding the time spent in backoff) by both successful and collided transmissions is the same. We denote this time by T_{Xmit}.

$$T_{Xmit} = T_{succ} = T_{coll} = T_{data} + T_{ack} + T_{mac\_overhead}, \tag{3.1}$$

where, T_{data} and T_{ack} denote the time required to transmit DATA packet and the ACK packet, respectively. $T_{mac\_overhead}$ is the time taken by MAC layer time delays like Distributed

[6]Details of Basic Access Mode and IEEE 802.11 Packet Formats and protocol details are provided in Section A.4 and Section A.2

Table 3.1: Notations used in the Analysis

Description	**Notation**
Number of contending nodes	N
Minimum congestion window	CW_{min}
Current backoff counter at node i	X_i
Maximum number of retries before a packet drop	M
Prob. of being in stage i of backoff	p_i
Prob. of collision in the network	P_c
Backoff time between 2 transmission attempts	Z_i^j
Backoff time between 2 successful transmissions	Z_i
Time for successful or collided transmission	T_{Xmit}
Time for a transmission attempt = $T_{attempt}$	$T_{Xmit} + Z_i^j$
Time between successful transmissions	μ

Interframe Space *(DIFS)*, Short Interframe Space *(SIFS)*, and the MAC layer headers[7]. The value for T_{Xmit} remains a constant for both collision and successful packets. For each transmission attempt, the nodes have to wait for a random amount of backoff time which is chosen using the Binary Exponential Backoff (BEB) algorithm. The time spent in backoff by the network is shown in Figure 3.2. Here, Z_i^j is the time spent in backoff for j^{th} attempt to transmit after the i^{th} successful transmission. Z_i is the time spent between two successful transmissions for the i^{th} interval.

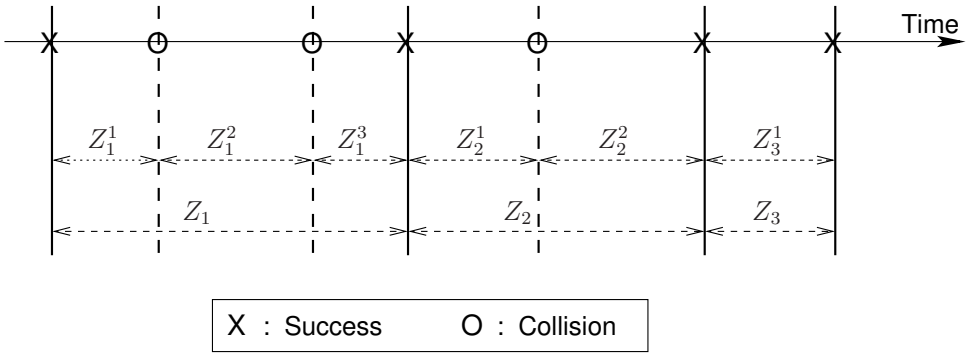


Figure 3.2: Aggregate Attempt Process at the MAC

Figure 3.2 shows the aggregate behavior of the MAC. Once the channel is idle, every node

[7]The IEEE 802.11 MAC timings are given in Section A.3

starts the backoff countdown simultaneously, the time interval Z_i^j represents the common time spent by all the contending nodes between two transmission attempts. We define, *residual backoff* as the pending backoff counter at any node while it attempts to transmit a packet. According to the IEEE 802.11 protocol [11], each contending node chooses a backoff value using the BEB algorithm . After the medium is idle for *DIFS* duration, the node starts decrementing the backoff counter with each time slot. The decrement operation continues till one of the contending nodes counts down to zero and starts transmitting. Once the medium is busy, the backoff counter for all the other contending nodes is frozen. After the current transmission is over, all nodes start the process of backoff count down again after the medium is idle for *DIFS*. The nodes which have a non-zero backoff counter when the counters were frozen in the previous contention attempt, reuse the backoff counter. Other nodes choose a fresh backoff counter depending on success or collision using the BEB algorithm. Thus, the backoff counter of a node at any given instance is the residue from the ongoing count-down process. We call this residue count as the *residual backoff* counter, and denote it by X_i for node i. The residual backoff counter helps us accommodate the delays experienced by a node due to transmissions by other nodes in the network as well. Now, the set $\{X_1, X_2, \cdots, X_N\}$ represents the residual backoff times of all N contending nodes in the network. The time spent in backoff by the MAC server shown in Figure 3.1, depends on the minimum backoff count among all contending nodes. Hence, we have,

$$Z_i^j \;=\; min\{X_1, X_2, \cdots, X_N\}. \tag{3.2}$$

Given that Z_i is the time spent in backoff between two consecutive successful transmissions, we have

$$Z_i = \sum_{j=1}^{C} Z_i^j, \tag{3.3}$$

where, there are a total of C transmission attempts between two successful transmissions. i.e., $(C-1)$ collisions and one successful transmission. If the probability of collision occurring in the network is given by P_c, then the probability of a successful transmission is $(1 - P_c)$. C is the count of transmission attempts occurring between two successful transmissions, and follows a geometric distribution (for $C = 1, 2, 3, \cdots$). Hence the expected value and variance of Z_i can be calculated as,

$$\begin{aligned} E[C] &= 1/P_c, \\ E[Z_i] &= E[Z_i^j] \cdot E[C], \\ Var[Z_i] &= (Var[Z_i^j] \cdot E[C]) + (E[Z_i^j]^2 \cdot Var[C]). \end{aligned} \tag{3.4}$$

The total time spent by the system between two transmission attempts is a combination of the time to transmit the packet and the time spent in backoff. Hence, from (3.1) and (3.2), we can write the time between two attempts as,

$$T_{attempt} = Z_i^j + T_{Xmit}. \tag{3.5}$$

As seen in Figure 3.2, there are $C - 1$ collisions and one successful transmission attempt that constitute the time between two successful transmissions. Hence, we can write the time between two successful transmissions, which is the service time of the IEEE 802.11 single cell MAC, as

$$\mu = E[C] \times E[T_{attempt}],$$

where, $E[C]$ denotes the expected number of transmissions (collisions + successful transmissions) and $T_{attempt}$, given by (3.5), is the time spent for each transmission attempt (backoff + transmission time). From (3.5) and (3.4), we can rewrite the the service time as

$$\mu = \left(E[T_{Xmit}] + E[Z_i^j]\right)/P_c. \tag{3.6}$$

The service time of the queuing system depicted in Figure 3.1 is given by (3.6). To calculate μ, we need to determine the values for Z_i^j and P_c.

3.1.2.1 Analysis of Backoff Times

From (3.2), the variables X_is denote the residual backoff times at individual nodes that are contending for access. We start with determining the distribution of the residual backoff value. In IEEE 802.11 MAC, the backoff counter is chosen to be uniformly distributed in the range $[0, 2^k CW_{min}]$, where k is the backoff stage. Calculating the residual backoff times for uniform

distribution is complex. We assume *Exponential* distribution for choosing the backoff value. In backoff stage k, the backoff counter is chosen to be from an exponentially distributed random variable with mean $2^k CW_{min}/2$. The result from [14] provides an analytical proof that the choice of distribution does not affect the aggregate performance of the MAC. We verify this behavior using QualNet [49] simulations. We compare the collision probability to verify the identical performance of Uniform and Exponentially distributed backoff times.

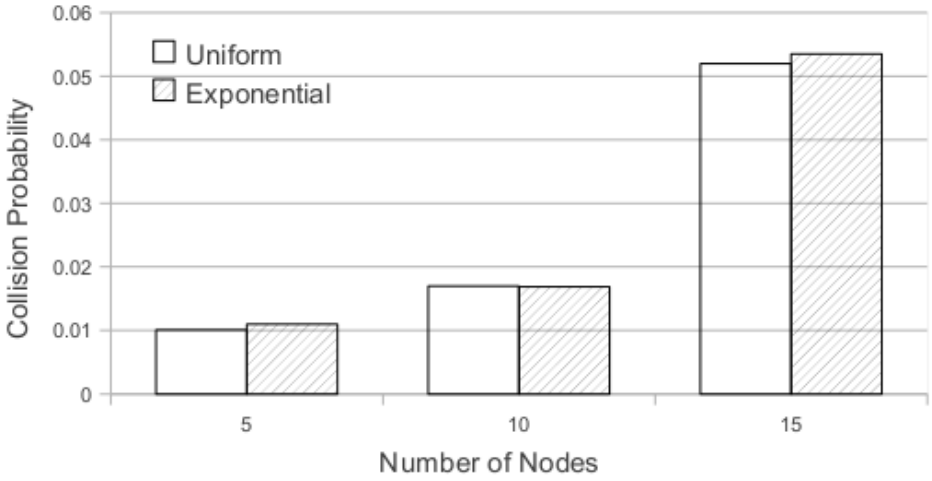


Figure 3.3: Collision Probability with Uniform and Exponential Backoff distributions.

Figure 3.3 shows the QualNet simulation results for 512 kbps arrival rate at each node. The simulations are performed for both Exponential and Uniform distributions being used for the backoff process. We perform the simulation by varying the numnber of nodes contending for channel access in the network. For different values of nodes in the network, it is observed that the results are identical for both Uniform and Exponential distribution in backoff.

The choice of Exponential distribution for backoff durations was done because of its "memoryless" property. Given an exponentially distributed variable R, the memoryless property states the following:

$$P[R > (s+t)|R > t] = \quad P[R > s] \quad \forall\, s,t > 0, \tag{3.7}$$

where, s and t are time instances during the attempt process, such that $s, t > 0$.

Due to the memoryless nature of the backoff times, the backoff counter remains exponential with the same mean even when the count-down freezes for channel busy periods. Hence,

from (3.7), we can write the equation for the value of backoff counter of node i while in backoff stage k as:

$$P[BO_i^k = x] = \left(\frac{2}{2^k \cdot CW_{min}}\right) e^{-\left(2/(2^k \cdot CW_{min})\right)x}. \tag{3.8}$$

Now, consider that the packet collision probability is P_c (derived in the next sub-section), then the probability of being in backoff stage k, denoted by the variable p_k, is given by the following set of equations:

$$\begin{aligned} p_2 &= P_c, \\ p_3 &= (P_c)^2, \\ \cdots &= \cdots \\ p_M &= (P_c)^{M-1}. \end{aligned}$$

Therefore, the probability of being in any stage k is given by the following equation

$$p_k = \quad (P_c)^{k-1} \quad 1 < k \leq M. \tag{3.9}$$

Also, we know that the sum of probability for all states is equal to one, $\sum_{k=1}^{M} p_k = 1$. Therefore, we can calculate the probability of being in stage 1 as follows:

$$\begin{aligned} p_1 &= 1 - \sum_{k=2}^{M} p_k \quad = \quad 1 - \sum_{k=1}^{M-1} P_c, \qquad \text{from (3.9)} \\ &= 1 - \frac{1 - (P_c)^M}{1 - P_c}, \\ &= \frac{(P_c)^M - P_c}{1 - P_c}. \end{aligned} \tag{3.10}$$

At any point of time, the node could be in one of the M backoff stages. We have information about the probability of a node being in stage k, from (3.9) and (3.10). We also know that the backoff value X_i is exponentially distributed in stage k, from (3.8). Thus, the distribution of residual backoff times turns out to be *HyperExponentially* distributed and can be written as:

$$\begin{aligned} X_i &\sim HyperExponential\Big(p_1, p_2, \cdots, p_M, \\ &\quad \frac{CW_1}{2}, \frac{CW_2}{2}, \cdots, \frac{CW_M}{2}\Big), \end{aligned} \tag{3.11}$$

and

$$\begin{aligned} P[X_i = x] &= P[BO_i = x], \\ &= f_{X_i}(x). \end{aligned}$$

where, $CW_k = 2^k \cdot CW_{min}$. Now, to calculate the value of parameter Z_i^j, from X_i, from (3.2), we need to find the first order statistic [50] for $\{X_1, X_2, \cdots, X_N\}$. The first order statistic is denoted by $X_{1:N}$.

$$\begin{aligned} Z_i^j &= min\{X_1, X_2, \cdots, X_N\}, \quad \text{from (3.2)} \\ \therefore Z_i^j &= X_{1:N}. \end{aligned} \tag{3.12}$$

Here, $E[X_{1:N}]$ will determine the average time spent by a cell in backoff before a transmission attempt. The corresponding variance is given by $Var[X_{1:N}]$. The individual variables, X_is are in turn dependent on the collision probability, it is complex to obtain the exact closed forms for the expectation and variance. Hence, we use the upper bounds for the expectation and variance. In [51], the authors show that the expectation of k^{th} order statistic is given by

$$E[X_{k:N}] = \mu' + \sigma\sqrt{\frac{k-1}{n-k+1}}.$$

where, μ' and σ are the Mean and Standard Deviation respectively, for identically distributed variables X_is.

The, residual backoff time, X_i, is *HyperExponentially* distributed as per (3.11). Hence, the mean and variance for X_i is given by

$$\mu' = \sum_{k=1}^{M}\left(p_k \cdot \frac{2^k CW_{min}}{2}\right), \tag{3.13}$$

$$\begin{aligned} \sigma^2 &= 2 \cdot \sum_{k=1}^{M}\Big\{p_k \cdot \left(\frac{2^k \cdot CW_{min}}{2}\right)^2, \\ &\quad - \left[\sum_{k=1}^{M} p_k \cdot \left(\frac{2^k \cdot CW_{min}}{2}\right)\right]^2\Big\}. \end{aligned} \tag{3.14}$$

Please note that μ' is not the same as μ which is the service time for the MAC. Now, we calculate the expected time between two transmission attempts Z_i^j as given in (3.12). Here, we need the first order statistic, i.e., for $k = 1$ in (3.13).

$$\begin{aligned} E[X_{1:N}] &= E[X_i] = \mu', \\ \therefore E[Z_i^j] &= \mu'. \end{aligned} \tag{3.15}$$

The authors show in [52], that the variance of the first order statistic is upper-bounded by the variance of the individual variables. The expression for variance of the first order statistic is given as:

$$\begin{aligned} Var[X_{1:N}] &< N \cdot Var[X], \\ \therefore Var[Z_i^j] &< N \cdot \sigma^2. \end{aligned} \tag{3.16}$$

Now, we have characterized Z_i^j required for the calculation of the MAC service time in (3.5) and (3.6). We need to determine the collision probability P_c to complete the analysis. We deal with the collision probability calculation in the next sub-section.

3.1.2.2 Calculating the Collision Probability

A collision occurs in the network when two or more nodes attempt to transmit at the same time instant. We assume that any collision event will not involve more than two nodes. This is commonly assumed for the analysis of random access protocols as the probability of more than two nodes involved in a collision is negligible. Hence, according to the model presented in the previous section, a collision will occur when the first and second order statistics for Z_i^j choose the same value, i.e., $X_{1:N} = X_{2:N}$. For all higher order statistics, the backoff counter will be non-zero when the transmission of the colliding nodes starts. The probability density function for the first and the second order statistic can be calculated using:

$$\begin{aligned} &P[X_{k:N} = x] = f_{X_{k:N}}(x), \\ &= n f_X(x) \cdot \binom{n-1}{k-1} \cdot F_X(x)^{k-1} \cdot [1 - F_X(x)]^{n-k}, \end{aligned} \tag{3.17}$$

where, $f_{X_i}(x)$ and $F_{X_i}(x)$ represent the probability density function and the cumulative distribution function of a HyperExponential random variable. The expressions for $f_{X_i}(x)$ and $F_{X_i}(x)$ are given by

$$F_{X_i}(x) = \sum_{k=1}^{M} p_k \cdot \left(1 - e^{-\left(2/(2^k \cdot CW_{min})\right)x}\right),$$

and

$$f_{X_i}(x) = \sum_{k=1}^{M} p_k \cdot \left(\frac{2}{2^k \cdot CW_{min}}\right) \cdot e^{-\left(2/(2^k \cdot CW_{min})\right)x}. \tag{3.18}$$

From (3.17), we calculate that the probability of a collision is given by

$$P_c = \int_{x=0}^{CW_{max}} P[X_{1:N} = x] \cdot P[X_{2:N} = x] \cdot dx. \tag{3.19}$$

3.1.2.3 Calculation of Service Times

Now, (3.18) and (3.19) lead to a fixed point formulation. These expressions do not give a closed form, hence we use MATLAB [53] to iteratively calculate the values for P_c. This value of P_c is then used to derive the values for service time of the MAC using (3.5) and (3.6). The service time of the MAC is nothing but the time taken for the the head-of-line packets at the contending nodes to be successfully transmitted. If we assume that each node gets fair share of the number of attempts to the MAC in the long run, then the access time for each node is $\frac{\mu}{N}$.

3.1.3 Validation of the Model using Simulations

In this section, we validate the results of the analysis with simulations. We perform simulations in QualNet Network simulator [49]. We consider a single-cell IEEE 802.11 based network for simulations. The parameters are given in Table 3.2.

As a continuously backlogged traffic source is not available directly in QualNet, we use a very high data rate Constant Bit Rate (CBR) source. The CBR source is configured to generate packets at an application layer data rate of 12 Mbps for an IEEE 802.11b network, resulting in saturation at each source. This ensures that the source has a packet to transmit in its queue all the time. The statistics regarding packet drops in the IP layer queue of a node are not collected. We also disable the Request to Transmit (RTS) [8] transmissions in QualNet by setting a high RTS threshold of 2312 bytes. Since, all packets transmitted are of 1500 bytes, no RTS is generated

[8] Details about the RTS packet in IEEE 802.11 standard are provided in further detail in Section A.2

Table 3.2: Parameters used in Simulations and for the Analytical Model

Parameters	**Values**
Cell size	250 x 250 meters
Number of nodes	200
Number of flows	10 to 100 in steps of 10
Packet size	1500 bytes
Channel Slot time	20 μs
Max number of retries (LRL)	7
Simulation time	300s
Duration of each flow	300s (Start:0s & End: 300s)

by the IEEE 802.11 MAC. We repeat the experiments five times and then average the results obtained in the individual runs.

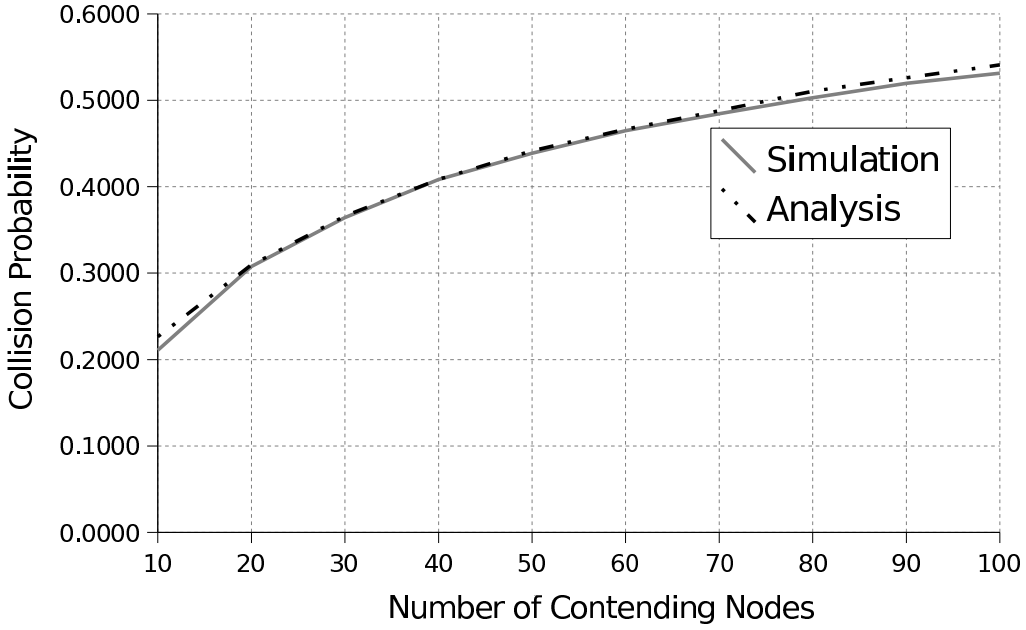


Figure 3.4: Packet collision probability in the cell

We record data packets collision statistics. In simulations, the ratio between the total number of ACK timeouts suffered at the MAC layer to the total number of packets transmitted gives the packet collision probability. The packet collision statistics are compared to the analytical results obtained using (3.19). Figure 3.4 shows comparison between analytical and simulation results. The results obtained from the analytical model match the results from simulations

closely.

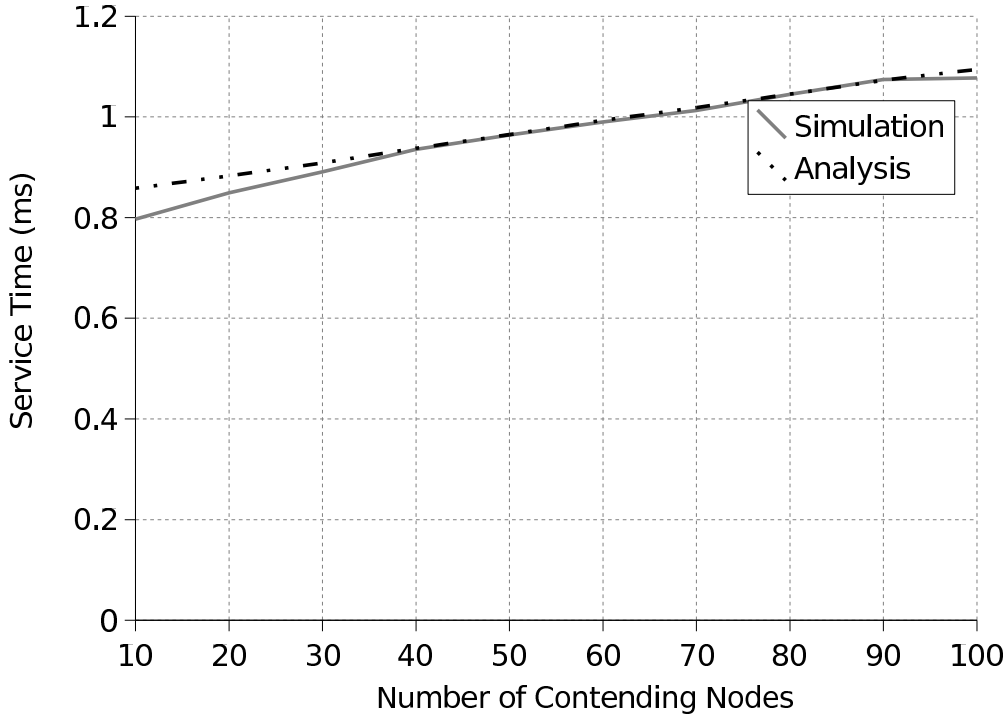


Figure 3.5: Service time of the MAC

We also record the time stamps for all packet transmissions in the simulation. The time difference between two transmission attempts gives the attempt time as calculated in (3.5). The time between two successful transmission attempts, as calculated in (3.6), was calculated to obtain the service time for the MAC. We calculate service time of the MAC for all the transmissions occurring in the network and calculate the average service time for each simulation run. Service times obtained for each simulation run are then averaged to determine the service time of the MAC. Figure 3.5 shows the comparison between simulation and analytical model. Here, we observe that the analysis matches the simulations closely and hence the model is validated.

3.2 Summary

In this chapter, we introduce the concept of an IEEE 802.11 cell as a network under consideration with one or more nodes attempting to transmit packet. Each individual node introduces packets into the wireless cell. In terms of a queue, the wireless channel is treated as a server and the MAC layer algorithm determines the processing delay before a packet at any of the nodes in the network is allowed to depart. We have also introduced the concepts for inter-exit time,

which is the time between two successful packet transmissions in an IEEE 802.11 cell. This same model will be used for the analysis in the rest of the thesis for the IEEE 802.11 network analysis.

In this initial analysis, we model the performance of an IEEE 802.11 cell in saturation conditions with the help of order statistics to determine the time taken by the head-of-line packets to be successfully transmitted (inter-exit time). Order statistic method allows us to determine the mean and variance of the inter-exit times with good accuracy without having to solve a detailed Markov chain for the IEEE 802.11 MAC. We observe that there is a good match between the analysis and QualNet based simulations.

In the rest of the thesis, we relax saturation assumption to determine the inter-exit-times. In the non-saturation case, we consider two possible scenarios for the network. Identical arrival rates at each node in the network, Homogeneous analysis in Section 4.1 and non-identical arrivals at the nodes in the network, Non-Homogeneous analysis in Section 4.2.

Chapter 4

Characterizing the Exit Process of IEEE 802.11 Wireless Network

The previous chapter has provided a prelimnary look at the analysis of an IEEE 802.11 cell and also introduced the network model under consideration. In this chapter, we consider the same network topology but with a more realistic traffic model. Specifically, we determine the time between two successful departures from an IEEE 802.11 network in the non-saturated case. Similar to the previous chapter, we consider a rural setup for deployment and hence ignore the effects of interference from other IEEE 802.11 networks.

There have been many performance analysis studies on IEEE 802.11 based networks. Kumar et. al. [14] and [54] study the performance of networks in the saturated conditions in 802.11 and 802.11e based networks. Other research works include analysis of the wireless network in a saturated condition or non-saturated but homogeneous traffic condition. However, to the best of our knowledge no existing research work provides a fixed-point model for non-saturated, non-homogeneous traffic in IEEE 802.11 based networks.

Initially, we discuss an approach to determine the time between two successful departures in a network with identical arrivals at each client node connected to the network, Homogeneous Arrivals. The analysis is performed using fixed-point theory to determine the distribution of time between two departure instances in Section 4.1. This analysis is further generalized to include Non-Homogeneous Arrivals in Section 4.2.

4.1 Homogeneous Traffic Arrivals in an IEEE 802.11 Wireless Network

In this section, we consider a non-saturated IEEE 802.11 based wireless network. We use a three-way fixed point to model the node behavior with Bernoulli packet arrivals and determine closed form expressions for the distribution of the time spent between two successful transmissions in an isolated network. The results of the analysis have been verified using extensive simulations in QualNet. The methodology presented in the section is novel and we believe that the analysis like ours can be used as an approximation to model the behavior of sub-components of a larger mesh or hybrid network.

4.1.1 Main Results

Consider a peer-to-peer system of n nodes communicating with each other using the 802.11 Medium Access Control (MAC) protocol. We are interested in the probability distribution function of the time between two successful transmissions in the network (as seen by an external observer). If all the nodes can listen to each other, then for our purpose, we can equivalently consider this network to be the uplink of a 802.11 cell with one Access Point (AP), n Customer Premises Equipments (CPEs), and no downlink traffic. From this point onwards, we refer to the network as an uplink of a cell. We assume that each node has a Bernoulli arrival of packets, which have to be transmitted to the AP. The packets received by the AP are handed over to the backbone mesh network for further forwarding and we are interested in modeling the probability distribution function of the time between two successful packet receptions by the AP.

The final justification for our simplifying assumptions and approximations is given by the close match of the analytical results with detailed QualNet simulations. We consider flows with an average arrival rate of 256 kbps, 512 kbps and 1 Mbps with the number of flows varying from 1 to 25. The IEEE 802.11b MAC is used in the simulations. Once the total load in the network reaches approx 5.5 Mbps, the network becomes saturated. Our analytical model matches accurately with the simulation results in the non-saturated as well as the saturated regime.

The system model is described in Section 4.1.2. In Section 4.1.3, we formulate the three-dimensional fixed point equation by accounting for the relationship between the System Time

and Backoff Time. We also compare our analytical results with detailed QualNet simulations. Section 4.1.4 derives the service time or inter-exit time distribution. This is also compared with QualNet simulations for different network loads.

4.1.2 System Description

We consider an IEEE 802.11 based wireless network. All nodes in the network are placed so that they are in the communication range of each other and employ a single channel for communication. Hence, one and only one transmission can occur in the network at a time. We define a *cell* as a geographical area containing the nodes in the wireless network. The cell contains n flows of uplink data traffic to the AP. The system model is shown in Figure 4.1 and 4.2. The nodes in the cell contend using the IEEE 802.11 MAC protocol.

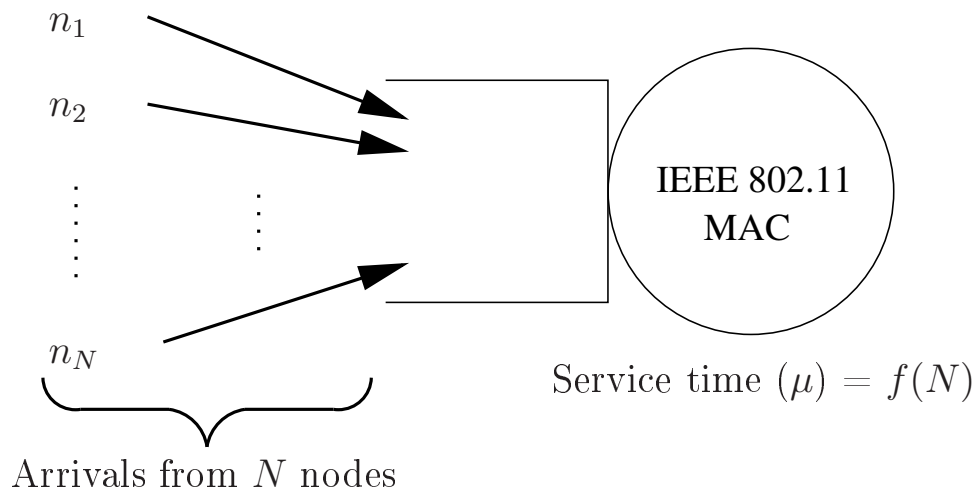


Figure 4.1: Model of a Single Cell Wireless Network with the MAC as Server

The IEEE 802.11 MAC based network is a slotted system. Nodes backoff for a random number of slots using Binary Exponential Backoff (BEB) algorithm before attempting to transmit. The backoff counter is decremented by one in every time slot. When the counter reaches zero, the nodes transmit. A time slot is the minimum unit of time defined in the IEEE 802.11 MAC and for IEEE 802.11b, it has a $20\,\mu$s duration. We assume that each node in the network has Bernoulli packet arrivals. The packets leave the node when a successful transmission occurs or the maximum number of retransmission attempts are exhausted.

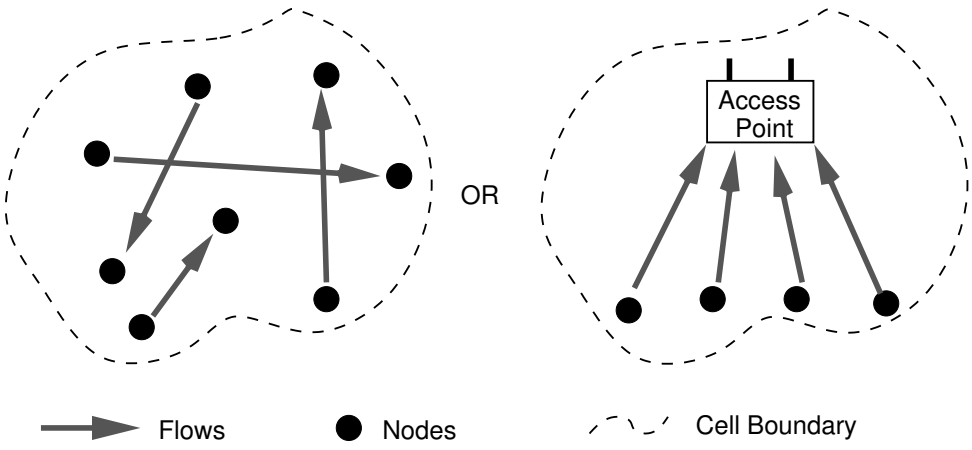


Figure 4.2: System Model. Both Peer-to-Peer and Access Point based uplink networks are equivalent for the sake of the analysis.

4.1.2.1 System Time and Backoff Time

In the previous Chapter, Section 3.1.2, shows the timeline in an IEEE 802.11 network in saturated conditions. In this section, we consider the same methodology to understand the System Time and Backoff Time. However, considering the network with non-saturated flows as compared to saturated flows, the number of active nodes at a given point of time is not constant. This difference is highlighted in the current section.

The aggregate attempt process at the MAC layer for a saturated network is shown in Figure 4.3. It can be seen that the channel activity periods (packet transmission and collisions) do not contribute to the backoff and attempt process of a node. Also, the total time spent in backoff by all the nodes is the same. This is because, during the channel activity periods all nodes in the network, except the ones transmitting packets, freeze their backoff counters. The aggregate attempt process for a non-saturated network is shown in Figure 4.4. Unlike the saturated case, the number of contending nodes changes as a result of packet arrivals during the channel activity periods and otherwise. As seen in Figure 4.4(a), node 3 is not backlogged in the beginning and it participates in the channel contention only after a packet arrival. Also in the process, node 1 clears part of its backlog and at a later point in time, when it has no backlog, it no longer participates in the channel contention. It can be seen that the backoff behavior of the nodes evolves on a time slot basis and the number of backlogged nodes changes on a much slower time scale. Hence, the number of contending nodes appears as a constant to the backoff process.

No transmission attempts are made during the channel activity periods, i.e., during packet transmissions. In the subsequent analysis, we consider *System Time* to represent the time spent

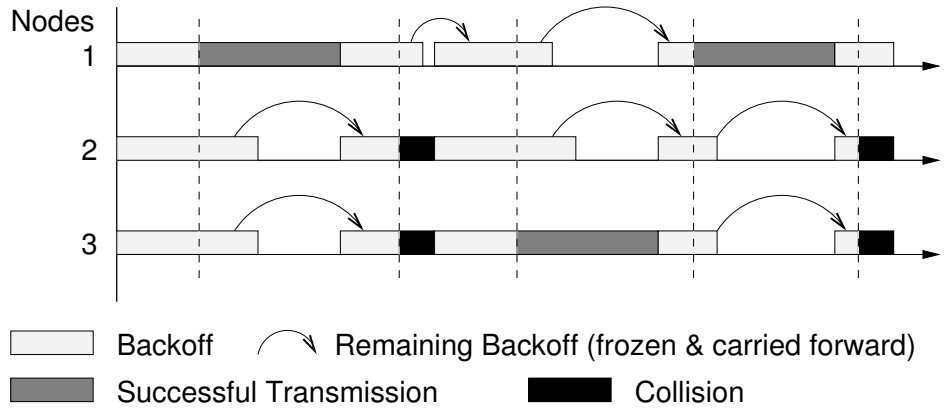


Figure 4.3: Aggregate Time of the System in Saturation. Backoff times are interspersed with Successful transmissions and Collisions.

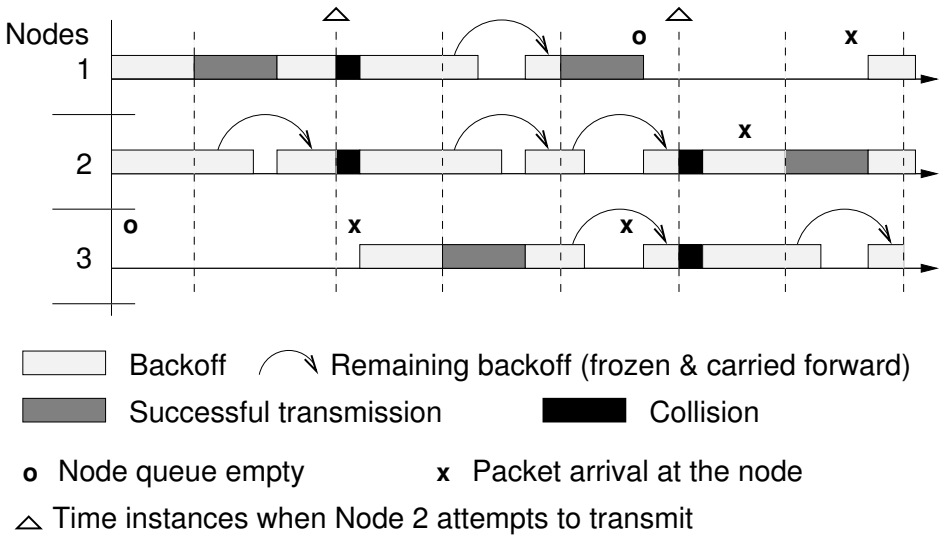
in channel activity (successful transmissions and collisions) and time spent in backoff as shown in Figure 4.4(a). The time during which the nodes backoff and count down to zero before transmissions is shown in Figure 4.4(b). Here, we have removed the channel activity periods and denote this time as the Backoff Time for the rest of the analysis. The network activity line in Figure 4.4(b) shows the result of the transmission attempts at backoff boundaries. From a node's perspective, as long as there is at least one packet in the queue, it will contend for channel access. Except for the number of backlogged nodes, the state of the nodes does not change outside the Backoff Time. Therefore, for analyzing the evolution of the states of the nodes, it is convenient to use the Backoff Time. However, for the analysis of the queue, we need the System Time. These two time scales are related through the random times spent in successful transmission and collisions. In our analysis, we account for this relationship.

4.1.3 Fixed Point Analysis of Non-Saturated Case

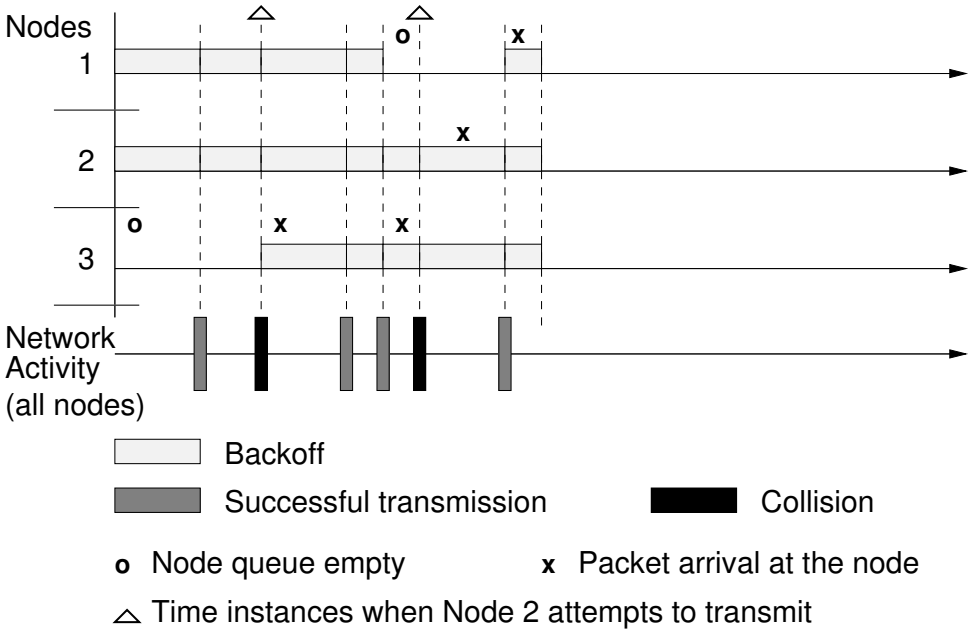
Since all the users have the same traffic arrival rate λ and all use the same MAC parameters, they have the same performance and we can study one representative user. In this section, our goal is to determine the following three quantities:

- $\beta =$ probability that a given user transmits;
- $\gamma =$ probability of collision given that a packet has been transmitted;
- $q_0 =$ probability that the queue of a given user is empty.

We derive their relationships and use them to numerically compute these quantities. In subsequent sections, these are used to derive the inter-exit time distribution. We note that while



(a) System Time



(b) Backoff Time, derived from the System Time shown above

Figure 4.4: Aggregate time of the system in a non-saturated network. The number of active nodes change depending on the queue lengths.

β and γ are determined by the dynamics during the Backoff Time, the queue evolves in System Time, and we need to account for these two times. The additional parameters required for this are summarized in Table 4.1.

Table 4.1: Notations used in Fixed Point Analysis

Description	Symbol
Number of contending nodes	n
Minimum contention window	CW_{min}
Maximum contention window	CW_{max}
Maximum number of retries for a packet	k
Effective arrival rate in Backoff Time	λ_{BO}
Slots required by successful transmission	T_s
Slots required by collision transmission	T_c

4.1.3.1 Calculation of Attempt Rate and Collision Probability

We follow the standard method of [14] with a variation to account for q_0, which is greater than zero in the non-saturated case. We derive expressions for β and γ in Backoff Time. Let R denote the number of attempts needed to transmit a packet and k be the maximum retries for a packet. Then the average number of attempts required to transmit a packet can be calculated as $\mathbf{E}[R] = 1 + \gamma + \gamma^2 + \cdots + \gamma^k$ and the average time spent in backoff before an attempt is $\mathbf{E}[X] = b_0 + b_1\gamma + b_2\gamma^2 + \cdots + b_k\gamma^k$. Here, $b_i = \frac{2^i CW_{min}}{2}$, for backoff stage i, where CW_{min} is the minimum contention window. The value for b_i is limited by the maximum number of retries (k) and the maximum contention window CW_{max}. After each transmission, the node repeats the procedure to transmit the packet. Hence, each attempt can be treated as an independent and identical process. The number of attempts to transmit, R, can be viewed as a 'reward' associated with the renewal cycle of length X [14]. Hence, the renewal reward theorem yields

$$\beta = \frac{1 + \gamma + \gamma^2 + \cdots + \gamma^k}{b_0 + b_1\gamma + b_2\gamma^2 + \cdots + b_k\gamma^k}. \tag{4.1}$$

Now, based on the decoupling assumption, the other backlogged nodes in the network attempt with a rate β independently of the given node. The probability that a node is backlogged is $(1 - q_0)$. The probability that an attempted transmission fails is

$$\begin{aligned} \gamma &= 1 - P(\text{None of the other } n-1 \text{ attempt}) \\ &= 1 - \sum_{l=0}^{n-1} \left[\binom{n-1}{l} q_0^{n-1-l} (1-q_0)^l (1-\beta)^l \right]. \end{aligned} \tag{4.2}$$

4.1.3.2 Calculation of q_0

The analysis of β and γ is based on the time spent only in the Backoff Time by nodes. The number of backlogged nodes is relevant for the backoff process only during the Backoff Time as shown in Figure 4.4(b). However, arrivals to the nodes can happen during the Backoff Time as well as the successful transmissions and collisions. So, the backlogged status of nodes changes due to arrivals that occur in the System Time as shown in Figure 4.4(a). Note that λ denotes the rate of arrival of packets in System Time and β and γ are calculated in Backoff Time. Hence, for the analysis of the queue lengths, we assume that all arrivals happen only during the Backoff Time. For this, we need to account for the arrivals occurring during channel activity periods and assume them to happen during the Backoff Time. We denote this effective arrival rate by λ_{BO}. By doing this, now we can analyze all the activity in the network in the Backoff Time. We next determine the effective arrival rate, which is then used to determine q_0.

As shown in Figure 4.4(a), let the constant time spent in a successful transmission and a collision be T_s and T_c respectively. If we consider a finite time window, then the relationship between the System Time and the Backoff Time depends on the random number of packet transmissions, failures and successes. To simplify the analysis, we consider the spirit of the "mean-field" approximation [29] - the aggregate behavior of the network as seen by a single user is replaced by the mean behavior. Thus, we use the conditional expectation of the System Time given the Backoff Time. The final justification for this step, as for our other approximations, is the close match we get with QualNet simulations. The conditional mean of System Time between two attempts = $(T_c \cdot$ Avg. No. of Collisions in y slots$) + (T_s \cdot$ Avg. No. of Successes in y slots$) + y$ slots, where y is the number of slots between two attempts in Backoff Time for the tagged node (see events marked with a triangle for node 2 in Figure 4.4). The number of attempts by all the other nodes is binomially distributed in y slots. The probability of attempt in each slot by any backlogged node is given by $1-(1-\beta)^{n^*}$, where $n^* = (n-1)\cdot(1-q_0)$ is the number of backlogged nodes in the network. (We note that we have once again replaced the number of contending users by the mean.) Hence, the mean number of attempts in y slots can be written as

$$L \;=\; y \cdot \left[1-(1-\beta)^{n^*}\right]. \tag{4.3}$$

There are, on an average, $\gamma \cdot L$ collisions and $(1-\gamma)\cdot L$ successes in the System Time between

two attempts by a tagged node. So the conditional mean of the System Time is given by

$$\begin{aligned}
&\big(T_c(\gamma \cdot L)\big) + \big(T_s(1-\gamma)L\big) + y \text{ slots} \\
&= L \cdot \big[T_c\gamma + T_s(1-\gamma)\big] + y \text{ slots} \\
&= \Big[\Big(1-(1-\beta)^{n^*}\Big)\Big(T_c\gamma + T_s(1-\gamma)\Big) + 1\Big]\, y.
\end{aligned}$$

Thus the conditional mean of the System Time given that the Backoff Time is y, is a multiple of y. We use this scaling factor to define the effective arrival rate:

$$\lambda_{BO} = \frac{\lambda}{\Big(1-(1-\beta)^{n^*}\Big)\Big(T_c\gamma + T_s(1-\gamma)\Big) + 1}. \tag{4.4}$$

Having determined the effective arrival rate, we now determine q_0. The queues at each node evolves as discrete time birth-death process. We have Bernoulli arrivals with rate λ_{BO} at each node. The packets leave the node on successful transmission. The probability of a birth is λ_{BO} and the probability of death (for nonzero queue length) is $\beta(1-\gamma)$. From [55], we obtain

$$q_0 = 1 - \frac{\lambda_{BO}(1-[\beta(1-\gamma)])}{\beta(1-\gamma)(1-\lambda_{BO})}. \tag{4.5}$$

Remark: Equations (4.1), (4.2), and (4.5) can be viewed a 3-dimensional fixed point equation in terms of β, γ, q_0. While Brouwer's fixed point theorem [56] gives the existence of a solution, in general the function involved is not a contraction. Hence to solve this equation we first fix a q_0, iterate between (4.1) and (4.2) several times to determine $\beta(q_0)$, $\gamma(q_0)$. Then we update q_0 using (4.5). This process is continued till numerical convergence is observed.

4.1.3.3 Determining Transmission Times: T_s, T_c

The parameters considered for computing the fixed overheads of T_s and T_c for successful transmission and collision are given in Table 4.2.

Since the calculations for β, γ, q_0 and λ_{BO} are in terms of time slots, we will convert the transmission and collision times to time slots. If a time slot is represented by τ, the respective number of slots for the transmission and collisions are as follows.

For Basic access mechanism (DATA-ACK):

$$\begin{aligned}
T_s = (1/\tau)\big(&T_{DIFS} + T_{PHY} + T_{DATA} \\
&+ T_{SIFS} + T_{ACK}\big) \\
T_c = (1/\tau)\big(&T_{DIFS} + T_{PHY} + T_{DATA} + T_{TO}\big)
\end{aligned}$$

Table 4.2: Time Consumed in IEEE 802.11 Packet Transmission

Description	**Time**
Packet Size for data flows	1500 Byte
PHY Data Rate of IEEE 802.11	11 Mbps
Slot time	20 µs
DIFS (T_{DIFS}) (1.5 slots)	50 µs
SIFS (T_{SIFS}) (0.5 slots)	10 µs
PHY Layer overhead (T_{PHY})	192 µs
Time to transmit RTS - 20 Byte (T_{RTS})	207 µs
Time to transmit CTS - 14 Byte (T_{CTS})	203 µs
Time to transmit ACK - 14 Byte (T_{ACK})	203 µs
Time to transmit DATA - (T_{DATA})	1112 µs
Time for CTS/ACK Timeout - (T_{TO})	408 µs

For Distributed Coordination Function (DCF) mechanism (RTS-CTS-DATA-ACK):

$$T_s = (1/\tau)\big(T_{DIFS} + T_{PHY} + T_{RTS} + T_{SIFS} + T_{CTS} + T_{SIFS} + T_{DATA} + T_{SIFS} + T_{ACK}\big)$$

$$T_c = (1/\tau)\big(T_{DIFS} + T_{PHY} + T_{RTS} + T_{TO}\big)$$

With the IEEE 802.11b parameters, these times are computed to be 78 and 88 slots for T_s and T_c respectively in Basic mode of access. In DCF mode of access, these times are 101 and 44 slots for T_s and T_c respectively.

4.1.3.4 Comparison with Simulations

In this section, we compare our analysis with simulations. The simulations have been performed in QualNet network simulator [49]. We consider a single-cell IEEE 802.11 based network for simulations. The parameters used are given in Table 4.3. We use the Variable Bit Rate (VBR) traffic generator of QualNet which generates traffic with Exponential inter-arrival times with the desired mean interval time. Static routing has been used in the simulations to avoid periodic routing updates initiated by the routing protocols. Hence, the only packets transmitted by the nodes are the ones generated by the VBR application. RTS threshold is set to the zero, so all packets being transmitted require a RTS-CTS exchange under the DCF mode of operation.

Table 4.3: Parameters used in Simulations and for the Analytical Model

Parameters	**Values**
Cell size	250 x $250\,\mathrm{m}^2$
Number of flows	1 to 25 in steps of 1
Packet size	1500 Byte
MAC	IEEE 802.11
PHY Data Rate	11 Mbps
RTS Threshold	0 Byte (for DCF mode)
Long Retry Limit (k)	7
Duration of flows	300 s (Start:0 s & End: 300 s)
Rate of each flow	256 kbps, 512 kbps and 1 Mbps

The slow convergence time of the queues can lead to bias in the statistics if the simulation duration is not large. To reduce the convergence time and expedite the simulations, we initialize the nodes with non-zero queue occupancy at the start of the simulation. We choose the distribution of initial queue length to be geometric with parameter $(1 - q_0)$ taken from the analytical model. This helps the queues reach steady state faster and with relatively shorter duration of simulation we get accurate results.

Statistics about packet transmissions, collisions, buffer occupancy at nodes and packet arrivals are collected during the simulations to obtain the collision probability and queue lengths. The queue length at each node is periodically logged for the entire duration of the simulation. At the end of the simulation, the number of instances of queue length being empty is divided by the total number of log entries to get the probability of queue being empty. All the packet transmission attempts are logged and the ratio of number of unsuccessful attempts to the total number of attempts by a node gives the collision probability.

The comparison of collision probability obtained from (4.2) and from simulations is shown in Figure 4.5. It can be seen from the figure that the collision probabilities rise rapidly after the number of nodes in the network increase beyond a certain threshold. On closer inspection, it can be seen that once the average aggregate arrivals to the network go beyond 5.5 Mbps, the collision probability increases suddenly. This is the saturation point of the network. It can be observed that the network reaches saturation at approximately 5 Nodes for 1 Mbps per node traffic. This can be observed for the other arrivals as well, 11 Nodes and 21 Nodes for 512 kbps per node and

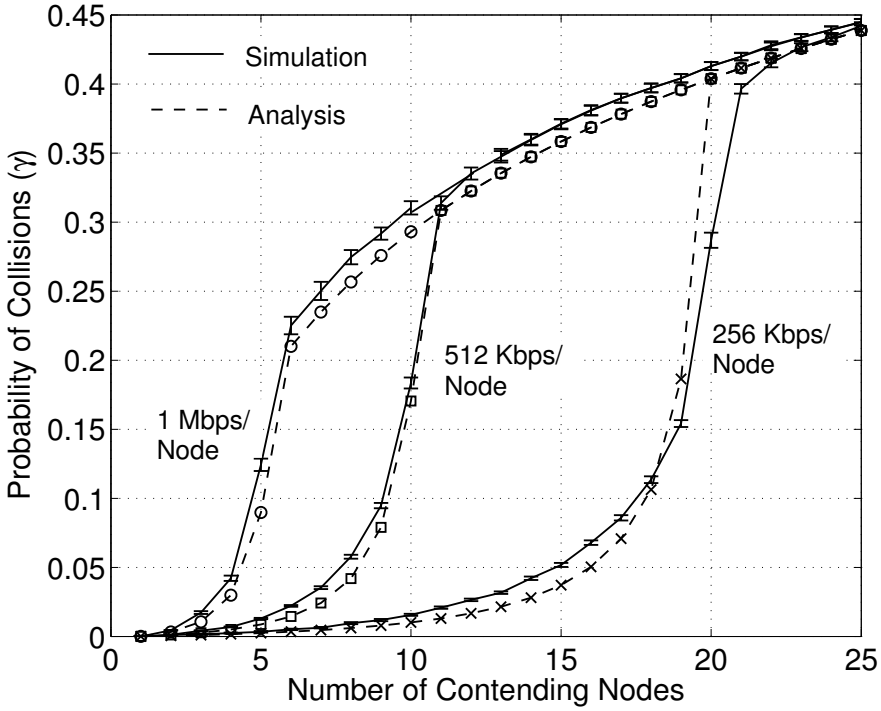


Figure 4.5: Comparison of Collision Probability for different arrival rates

256 kbps of traffic per node respectively. Hence, for 1500 Byte packets, the saturation condition of the network is dominated by the aggregate traffic in the network and not by the number of contending nodes in the network. There is a close match between the simulation values and the values obtained from analysis. The expressions for γ, β and q_0 are not valid once the network reaches saturation condition as the queue becomes unstable (i.e., total arrivals are more than the total departures). Hence, in the saturation condition, the analysis degenerates to a simple saturation case analysis without queues as given in [14].

The collision probability observed for smaller packet sizes is shown in Figure 4.6. We fix the arrival rate of traffic to 256 kbps per node and vary the size of packets. It can be seen that even though the arrival rate is the same, smaller packet sizes lead to saturated network condition sooner. This happens as a result of heavy contention in the channel at smaller packet sizes. When smaller packet sizes are used keeping the data rate constant, the rate at which individual packets arrive at the queue increases. This leads to more frequent attempts to transmit in the network. This increased contention in the network leads to early saturation condition. It should be noted, that in the case with different packet sizes, the overheads associated with collisions dominate the saturation effect.

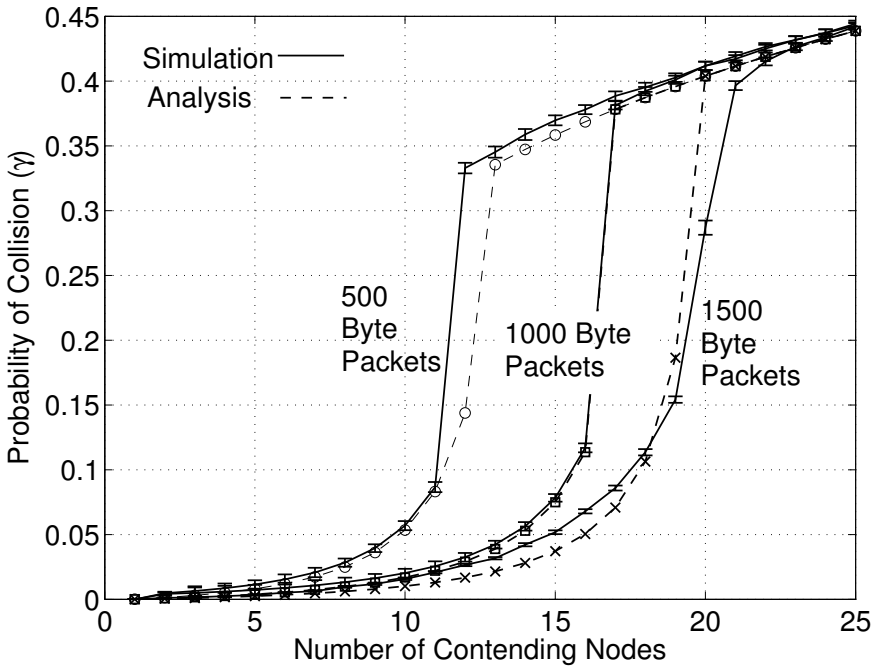


Figure 4.6: Comparison of collision probability for varying packet sizes at 256 kbps traffic per node

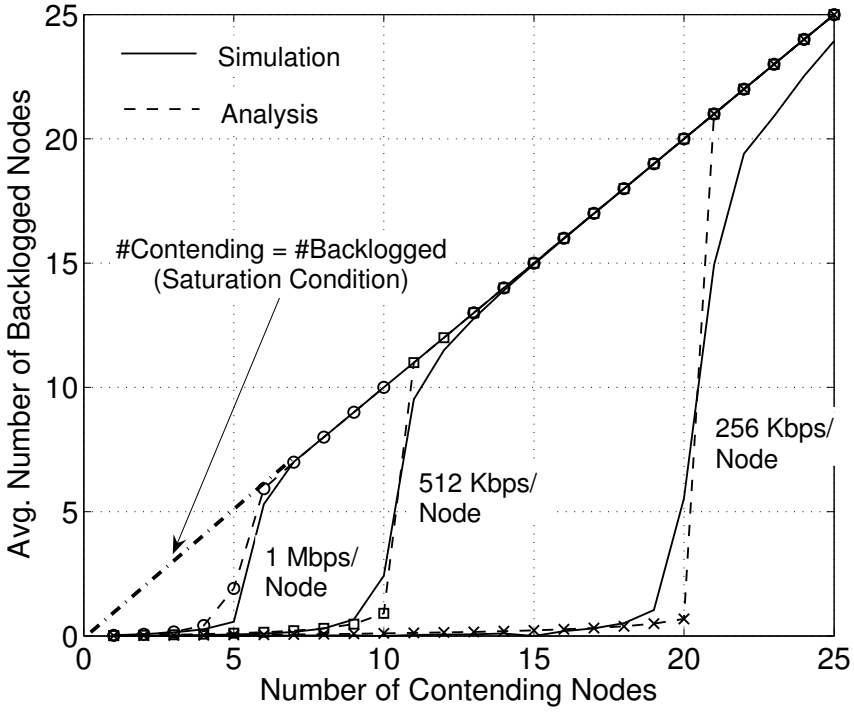


Figure 4.7: Average Number of Backlogged Nodes for different Arrival Rates

Figure 4.7 shows the average number of backlogged nodes in the network at any given

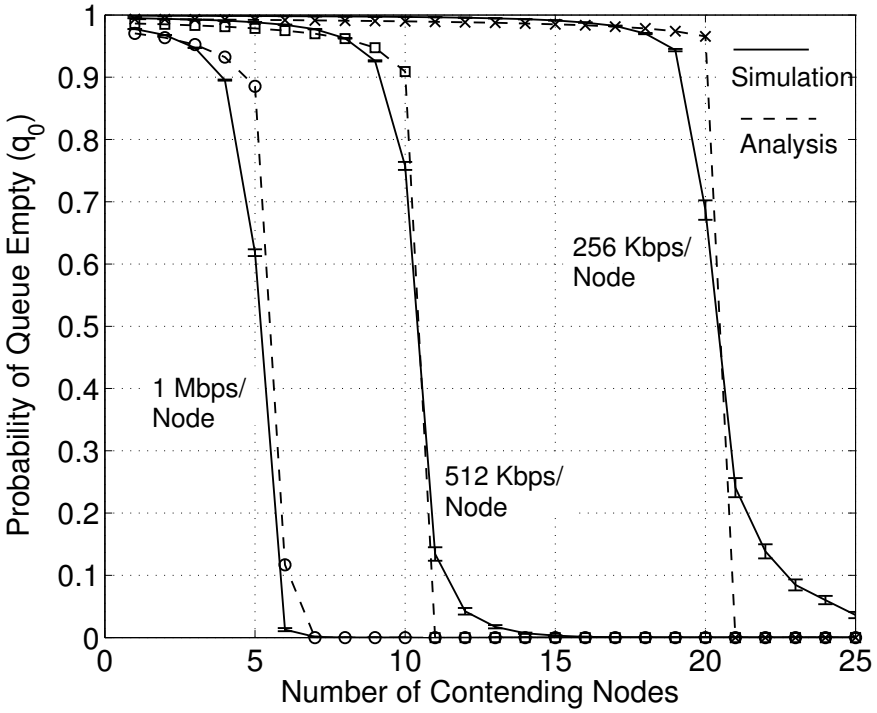


Figure 4.8: Comparison of Probability of Queue Empty for different arrival rates

point of time. This number is calculated as

$$\text{Average Num. of Backlogged Nodes} = n(1 - q_0),$$

where q_0 is from (4.5). The network is in saturation condition if the average number of backlogged nodes is equal to the number of contending nodes. It can be seen that for higher loads, the network reaches saturation sooner as compared to lightly loaded flows. This confirms the observation that the network is capacity limited by the aggregate arrivals and not by the number of nodes. We can use this result as noted in [15] to determine the TCP throughput by replacing the number of nodes in the network by the average number of backlogged nodes and performing a saturation analysis.

Figure 4.8 shows the probability of the queue being empty as the number of nodes in the network increases for different arrival rates. It can be observed, that the queues remain empty with probability more than 0.9 till the network reaches the saturation point. Once the saturation point is reached, the probability of queue being empty rapidly drops and stabilizes at 0. The analytical model developed by us is able to track the behavior of the queues accurately in the non-saturated region.

The comparison between the analysis and simulation results for Basic Access Mechanism

follow the same trend. Apart from the times T_s and T_c for successful transmissions and collisions, the rest of the analysis remains the same.

4.1.4 Exit Process of an IEEE 802.11 Cell

The exit process of an IEEE 802.11 cell is the time observed by an external entity between two successful packet transmissions in the cell irrespective of the source node. This definition is different from the service time of a node.

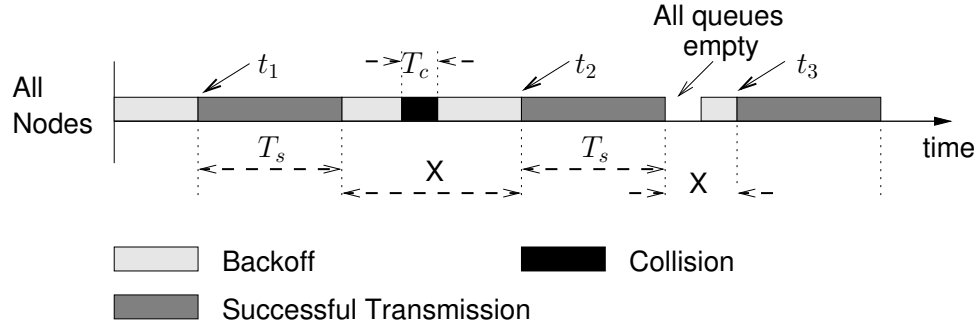


Figure 4.9: Time between two successful transmission attempts at Node 1.

As illustrated in Figure 4.9, we are interested in the time intervals $(t_2 - t_1)$ and $(t_3 - t_2)$. It can be noted that the the minimum time between two successes is T_s, i.e., the time associated with the transmission of a successful packet. Also note that between two successful transmissions, there could be zero or more collisions. The other overheads include the time consumed in backoff count-down, collisions occurring in the network, and the time for which all queues in the network are empty. Hence, the exit time is $T_s + X$, where X represents the time spent because of backoff, collisions and idle time when all queues are empty. In Section 4.1.4.1 we derive expressions for $P(X = x)$ and compare them with QualNet simulation in Section 4.1.4.2.

4.1.4.1 Derivation of $P(X = x)$

Let A be the event that no node is backlogged. Then $P(A) = q_0^n$ and we write

$$\begin{aligned} P(X = x) = q_0^n P(X = x|A) \\ + (1 - q_0^n) P(X = x|A^c). \end{aligned} \tag{4.6}$$

When there is no backlog, the next transmission occurs as soon as a packet arrives. Thus

$$P(X = x|A) = \psi(1 - \psi)^{x-1}, \quad \psi = 1 - (1 - \lambda)^n. \tag{4.7}$$

So we only have to determine $P(X = x|A^c)$. We note that

$$P(X = x|A^c) = \sum_{i=1}^{\infty} P(X = x, S_i|A^c), \tag{4.8}$$

where S_i is the event that there are $i - 1$ failures before the success. The probability of attempt by at least one node in the network in a time slot is

$$\begin{aligned} \phi &= P(\text{Atleast one attempt}), \\ &= 1 - P(\text{No attempts}), \\ &= 1 - \sum_{l=0}^{n} \binom{n}{l} q_0^{n-l}(1 - q_0)^l(1 - \beta)^l. \end{aligned} \tag{4.9}$$

Then

$$\begin{aligned} P(X = x, S_0|A^c) &= \phi(1 - \phi)^{x-1}(1 - \gamma) \\ P(X = x, S_1|A^c) &= (x - T_c - 1)\phi(1 - \phi)^{x-T_c-1}\gamma \\ &\quad \times \phi(1 - \phi)^{T_c-1}(1 - \gamma) \\ &= (x - T_c - 1)\phi^2(1 - \phi)^{x-2}\gamma(1 - \gamma). \end{aligned} \tag{4.10}$$

Since γ is usually small, we ignore the higher order terms in (4.8) and approximate $P(X = x|A^c)$ just with the above two terms. Thus from (4.6), (4.7), (4.8), and (4.10), we get a simple approximation to $P(X = x)$.

Now, the inter-exit time distribution is given by $T_s + X$, T_s is the constant time incurred in successful transmission of a packet, and X has probability law derived above. Our analysis is valid for both basic access mechanism as well as the DCF mode of operation of IEEE 802.11 MAC protocol. Since the different exit times are independent and identical, this characterizes the exit process.

4.1.4.2 Comparison with Simulations

The time stamps for all packet transmission attempts are collected during the simulations to obtain exit times. The time between two successful transmissions is recorded as exit time. Since, all the analytical derivations are based on a slot time scale, we convert the exit time to slots. At the end of the simulation, the time between consecutive successes is computed and divided by the slot time ($20\,\mu$s) to obtain the exit times in terms of time slots.

Figures 4.10 and 4.11 illustrate the comparison between analysis and simulation for cumulative density function (CDF) of the exit times. The simulations have been performed for DCF

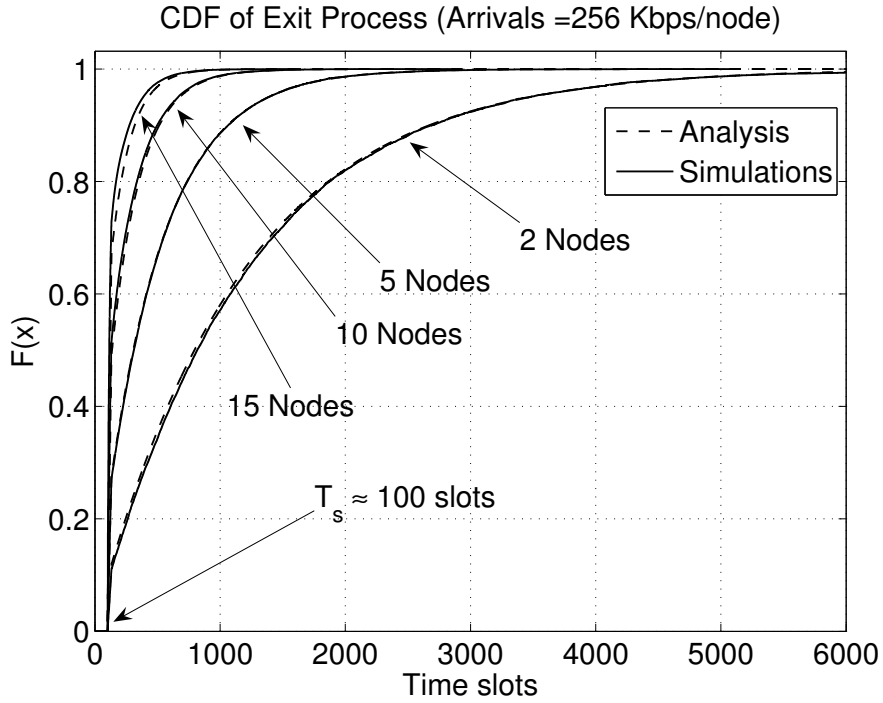


Figure 4.10: Comparison of Exit Time Distribution for varying number of contending nodes. Each node has an arrival rate of 256 kbps.

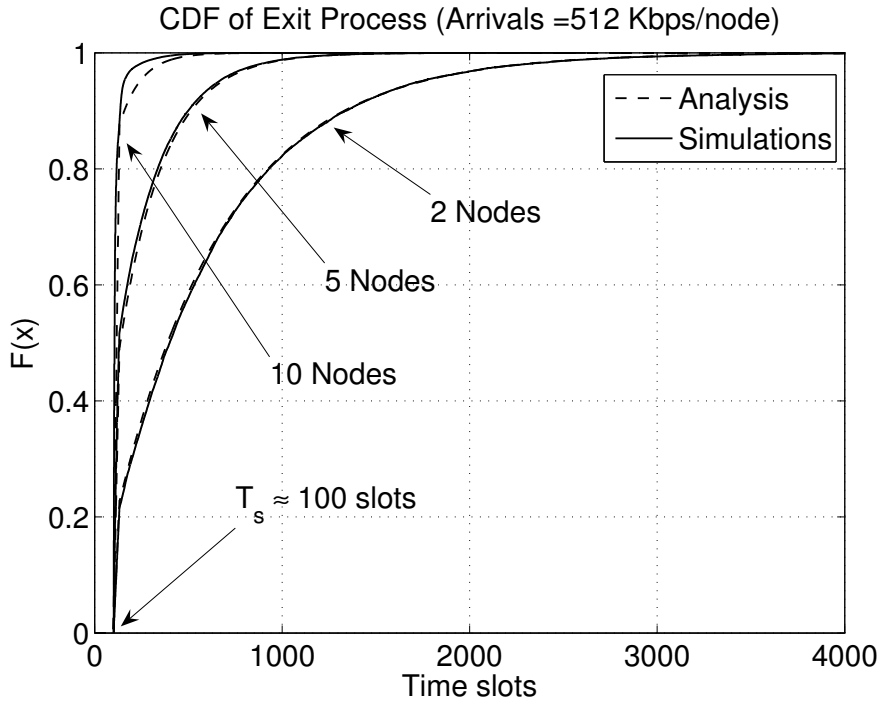


Figure 4.11: Comparison of Exit Time Distribution for varying number of contending nodes. Each node has an arrival rate of 512 kbps.

mode of operation. It can be observed that as the number of nodes in the network increases, the network spends more time in the backlogged phase $(w.p.\ 1 - q_0^n)$, and lesser time in the

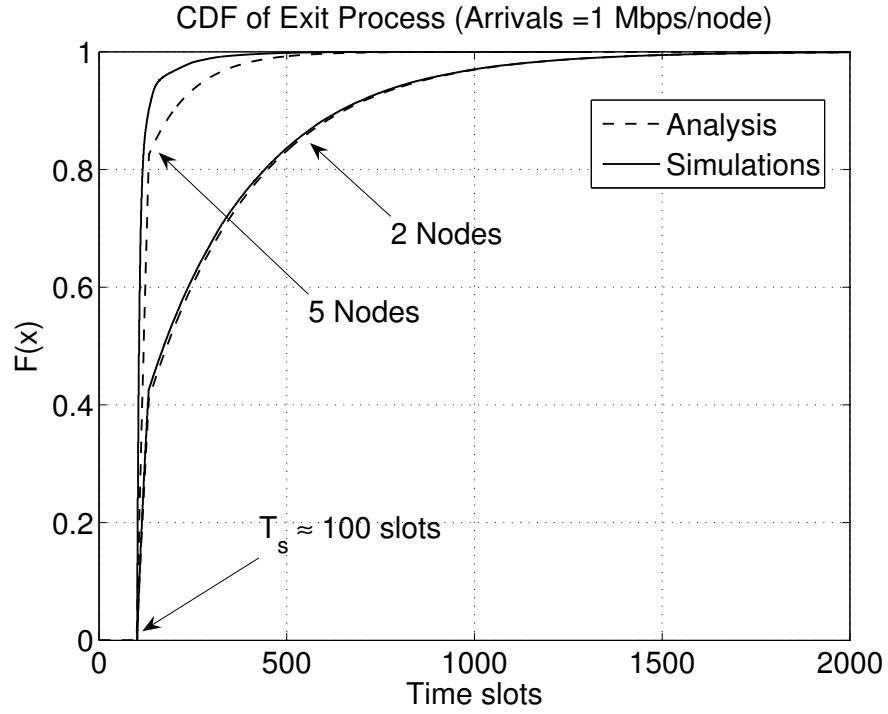


Figure 4.12: Comparison of Exit Time Distribution for varying number of contending nodes. Each node has an arrival rate of 1 Mbps.

idle phase waiting for packet arrivals $(w.p.\ q_0^n)$. Since the constant overhead for a successful packet transmission is 101 slots in DCF, the observed CDF has a constant minimum overhead of roughly 100 slots between two successes. It can also be noted that the network reaches near saturation condition for fewer number of nodes in the case of 512 kbps per node arrival rate, i.e., 10 nodes instead of 15 nodes in case of 256 kbps per node.

Figure 4.12 illustrates the CDF for arrival rate of 1 Mbps per node. It can be seen that the network spends most of the time in backlogged phase and channel contention and less idle time even for very few nodes. This observation is in agreement with the saturation conditions observed in Figure 4.7. It can also be observed that at higher arrival rates, the maximum time spent in the idle state waiting for packet arrivals is reduced from 6000 slots for 256 kbps/node traffic to 2000 slots for 1 Mbps/node traffic.

4.2 Non-Homogeneous Traffic Arrivals in an IEEE 802.11 Wireless Network

In this section, we use a multi-way fixed point formulation to analyze the performance of a Non-Homogeneous IEEE 802.11 based wireless network with each node having a Bernoulli packet arrival process. We determine the probability of collision in the network and the probability that a node is backlogged. These results are then verified using simulations in QualNet.

We consider a single cell IEEE 802.11 based wireless network. The network consists of n wireless nodes connected to an access point. Traffic arrival at each node is Bernoulli. This is an extension to the results in Section 4.1, where we consider arrivals to each node is equal and identical. The system model considered is the same as the Homogeneous Arrivals case, as shown in Figure 4.2.

This analysis can be developed further to determine the distribution of time between two packets from a wireless cell. Such an analytical model will be very useful in speeding up both simulation and testbed based evaluation of complex networks where departures from a smaller wireless network can be replaced by this model.

4.2.1 Fixed Point Analysis of Non-Saturated, Non-Homogeneous Case

In Section 4.1, we have derived a fixed-point approach to determine the collision probability (γ), queue empty probability (q_0), and attempt rate (β) for each node. In the Homogeneous case, γ, β and q_0 are identical for each node.

The set of equations in the fixed-point from (4.1), (4.2) and (4.5) are:

$$\begin{aligned}
\beta &= \frac{1+\gamma+\gamma^2+\cdots+\gamma^k}{b_0+b_1\gamma+b_2\gamma^2+\cdots+b_k\gamma^k}, \\
\gamma &= 1-\sum_{l=0}^{n-1}\left[\binom{n-1}{l} q_0^{n-1-l}(1-q_0)^l(1-\beta)^l\right], \\
q_0 &= 1-\frac{\lambda_{BO}(1-[\beta(1-\gamma)])}{\beta(1-\gamma)(1-\lambda_{BO})}.
\end{aligned}$$

Here, $\lambda_{BO} = \lambda \cdot \Big([1-(1-\beta)^{n^*}][T_c\gamma + T_s(1-\gamma)]+1\Big)$, $b_i = \frac{2^i CW_{min}}{2}$ is the mean backoff time for backoff stage i. b_k is limited by the maximum number of retries k before dropping a packet. n is the number of nodes in the network, and $n^* = (n-1)\cdot(1-q_0)$ is the avg. number of backlogged nodes in the network. T_s and T_c are the constant time overheads involved with the

successful transmission of a packet and a collision respectively. Note here that γ, β and q_0 are evaluated in Backoff Time where all overheads of channel activity periods are ignored. λ_{BO} is the scaled arrival probability λ to keep track of arrivals in System Time (actual real world time) and convert them into the Backoff time equivalent.

We continue to use the two time scale (Backoff Time, System Time) approach from Section 4.1 for the Non-Homogen-eous traffic case. In this case, queues at each node behave independently and hence, the attempt rates (β_i) at each node will be different. So, the set of fixed point equations can be represented as a vector of equations, where a 3-tuple ($\beta_i, \gamma_i, q_{0i}$) of equations denotes the behavior of each node. We continue to analyze the system from the perspective of a single node i.

4.2.1.1 Calculation of Attempt Rate and Collision Probability

A collision in Backoff time is said to occur when a given node i transmits in a time slot, and at least one more node transmits in the same time slot. Given each node has a different arrival rate, queues at each node will be backlogged independently. Hence, the total possibilities in which nodes in the network can be backlogged can be represented as a power-set of nodes. If N is the set of all nodes, $\mathcal{P}(N-i)$ is the power-set of the set of all nodes in the network except node i. Now, the collision probability and attempt rate can be written as:

$$\beta_i = \frac{1+\gamma_i+\gamma_i^2+\cdots+\gamma_i^k}{b_0+b_1\gamma_i+b_2\gamma_i^2+\cdots+b_k\gamma_i^k} \tag{4.11}$$

$$\begin{aligned}\gamma_i &= 1-\text{Prob}\{\text{No backlogged node attempts}\} \\ &= 1-\sum_{B\in\mathcal{P}(N-i)}\Big(\prod_{j\in B}(1-q_{0j})(1-\beta_j)\prod_{j\notin B}q_{0j}\Big)\end{aligned} \tag{4.12}$$

4.2.1.2 Calculation of q_{0i}

Packets arrive at node i in the System time with the probability of arrival λ_i in a time slot. Given two time instances t_1 and t_2, the total possible overhead (time spent in successful packet transmissions and collisions) by node j in each Backoff slot is given by : Probability of non-collided attempt $\times$ No. of slots used in channel activity, i.e., $\beta_j(1-q_{0j})[T_c\gamma_j+T_s(1-\gamma_j)]$. Hence, relation of arrival rate in Backoff time to arrival rate in System time can be written as

$$\lambda_{BOi}=\lambda_i\Big(1+\sum_{j=1}^{n}\beta_j(1-q_{0j})[T_c\gamma_j+T_s(1-\gamma_j)]\Big).$$

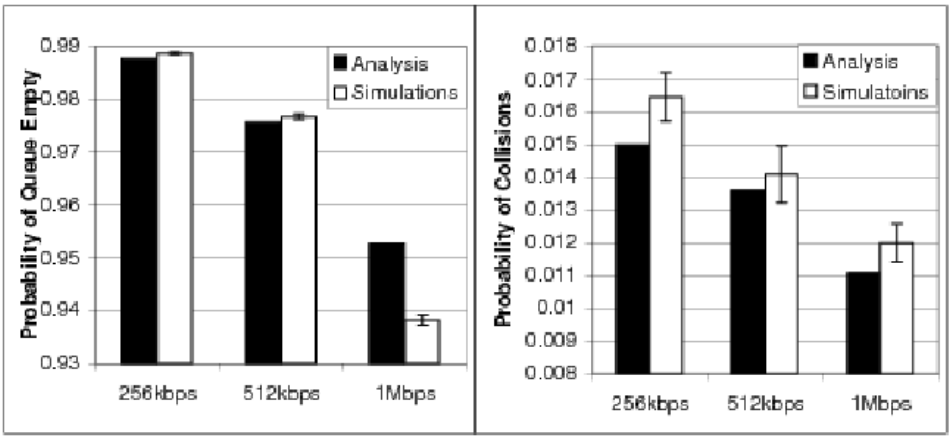


Figure 4.13: Probability of queue empty and collision probability for a Non-Homogeneous scenario

Hence, the probability of queue being empty is

$$q_{0_i} = 1 - \frac{\lambda_{BOi}(1 - [\beta_i(1 - \gamma_i)])}{\beta_i(1 - \gamma_i)(1 - \lambda_{BOi})}. \tag{4.13}$$

Remark: Equations (4.11), (4.12) and (4.13) represent a set of fixed point equations for node i. Hence, for a system of n nodes, we have a fixed point system in 3 $\times n$ equations or a vector of 3 equations.

4.2.2 Validation of the Analysis

We verify the analytical model derived in the previous section with simulations in QualNet simulator. The important simulation parameters used in QualNet are as follows: Simulation duration - 300 s, MAC Protocol - IEEE802.11b, Retry limit - 7, Cell size - 250 m $\times$ 250 m, Packet size - 1500 Byte. All simulations are run for 5 different seed values and results are plotted with 95% confidence interval.

Figure 4.13 shows the comparison of simulations with analysis for a scenario with the following setup: 4 Nodes-256 kbps, 2 Nodes-512 kbps, 1 Node-1 Mbps. It can be seen that the results for the analytical model match well with the simulation results. In this case the aggregate arrival rate in the network is 3 Mbps which is less than the saturation limit (approx 5.5 Mbps). We observe that the probability of collisions experienced by a node with 256 kbps and 512 kbps arrival rate nodes is higher than the node with 1 Mbps. Also, the probability of queue empty for 1 Mbps node is lower than the 256 kbps and 512 kbps nodes. This could be because of short-term unfairness introduced by the 1 Mbps flow.

4.3 Summary

In this chapter, we have presented the analysis of an IEEE 802.11 network cell in both the homogenous arrivals and non-homogenous arrivals case. In the homogeneous arrival case, where all nodes in the network have identical arrival rates, we determine a closed form expression for the inter-exit-time distribution. We also demonstrate with the help of simulations that the obtained expressions are accurate in predicting the inter-exit-times. We extend the network model for non-identical arrival rates for nodes in the network and determine average values for collision probabilities. With the help of simulations in QualNet, we demonstrate that the results obtained with non-homogeneous arrival analysis are accurate.

Chapter 5

Experimental Validation of IEEE 802.11 Analysis

In this chapter, we discuss setting up of the IEEE 802.11 testbed and validate the results from the analytical modeling in Chapter 4. Validating the analytical model for IEEE 802.11 on a practical network has several key considerations. The analytical model makes certain simplifying assumptions regarding the traffic pattern, i.e., Poisson arrival process with different arrival rates at each node. We have considered both homogeneous arrivals and non-homogeneous arrivals in Sections 4.1 and 4.2 respectively. Given this consideration on the analytical model, it would be difficult to gauge the accuracy of the analytical model as compared to measurements from the IEEE 802.11 testbed without studying both the cases using the same set of parameters. Hence, we have used an isolated IEEE 802.11 network with traffic generators to introduce traffic load in the network.

5.1 Setting up an IEEE 802.11 Testbed

We consider a 10 node testbed in an indoor laboratory. Several factors are considered during the setup of the testbed:

1. Choice of workstations,

2. Choice of network interfaces on the workstations,

3. Choice of wireless cards to be used on the workstations,

4. Choice of the wireless access point to be used in the testbed, and

5. Choice of tools to be used for monitoring and measurement.

In this section, we address the various factors involved in the decision making of choosing components of the testbed. For the choice of the workstation and operating system platform, Linux was a straight forward option because of the inherent flexibility of open source software. The ability to modify and customize certain aspects of the wireless driver is specified in further detail in Section 5.1.2 of this chapter. In addition to that for the purpose of easy control of the experiment parameters, start-stop times, and measurements, each workstation in the testbed had two network interfaces, one being the wireless interface being used to perform the controlled transmissions and measurements of the IEEE 802.11 protocol, second being a wired network interface for controlling the experiments. This particular aspect of the workstation is discussed in further detail in Section 5.1.1 and 5.2.2.

The choice of the wireless card has been made depending on the following factors 1) Full source code availability of Linux drivers without dependence on closed source binaries 2) Detachable antenna support 3) Monitor Mode support. Each of these capabilities of the wireless card is deemed important for utilizing the card to the maximum extent possible in the testbed. For the purpose of performing controlled experiments, we need to make modifications in the wireless card driver as mentioned in Section 5.1.2. The section also discusses the need for modifications to the wireless driver. An external antenna on the wireless card provides flexibility in adding Radio Frequency (RF) attenuators and high gain external antennas whenever needed in order to control the range of the interference in the testbed. The external antenna, though not a very strict requirement, provided flexibility to the hardware that could be used in the testbed. Monitor mode support on the wireless card is essential when performing packet capture using the interface. In the packet capture mode, the *libpcap* library used by the tool *Wireshark* [57] uses the generic layer 2 packet header when a packet capture is performed on a wireless interface in the regular transmit-receive mode. This also does not capture any of the IEEE 802.11 specific control packets like RTS, CTS, ACK [9] In the monitor mode, the IEEE 802.11 packet header is captured by the *libpcap* library along with all the other control packets. This behavior is important for the purpose of measurements in the testbed. Based on these parameters, the desktop machines are used with a TP-Link TL-WN350GD PCI card [58] to provide WiFi

[9]Further details of the packets and relevance to the IEEE 802.11 protocol is provided in A.2.

Table 5.1: Wireless Card Details

Hardware	Details
Wireless Card	TP-Link TL-WN350GD PCI card
Wireless Chipset Chipset	Atheros AR2417
PHY Data Rate	54 Mbps
IEEE Standards	IEEE 802.11 b/g capable
Frequency Range	2.4 GHz
Antenna Connector	Reverse Polarity - SubMiniature version A (RP-SMA)
Maximum Output Power	18 dBm
External Antenna	2 dBi

connectivity. The specifications for the wireless card used in the setup are given in Table 5.1.

The card being used in the testbed is based on a widely known Atheros chip, that has good open source support for drivers. In addition to the wireless drivers, the card has support for external antenna and a PCI interface.

All the nodes in the testbed were associated to a Linksys WRT54GL [59] wireless router [10] with *OpenWrt* [60] operating system loaded. OpenWrt is a Linux distribution for embedded devices that supports all the basic Linux commands and utilities to run on devices with very limited compute power and memory. The OpenWrt embedded operating system also provides the ability to install user specified programs with a quick and easy porting method to run on the embedded device.

An open source operating system was chosen on the wireless router for gaining command line access to the router machine and enabling on-demand statistic collection from the router which is difficult to achieve using the factory default firmware of the wireless router.

5.1.1 Network Topology

Every node in the network has two interfaces; a 10/100 Fast Ethernet interface for control operations like start-stop generating traffic and start-stop recording statistics and a wireless interface for the wireless traffic in the network testbed. A basic control protocol is implemented using

[10] A wireless router provides all functionality of an IEEE 802.11 access point. The wireless router typically has a wide are network (WAN) interface in addition to the local area network (LAN) interfaces. For all practical purposes, discussion in this chapter uses the term access point and wireless router interchangably.

socket programming on Linux to handle basic operations of start/stop of the traffic flows and capture wireless packet traces. Broadcast packets are used in order to issue control commands to all the nodes in the testbed.

From a network topology perspective, all nodes are connected to the same switched network on the Ethernet interface. This ensures that there is minimal delay in the transmission of the control packets to the nodes (except queuing delay). Figure 5.1 illustrates the network connectivity diagram for the testbed.

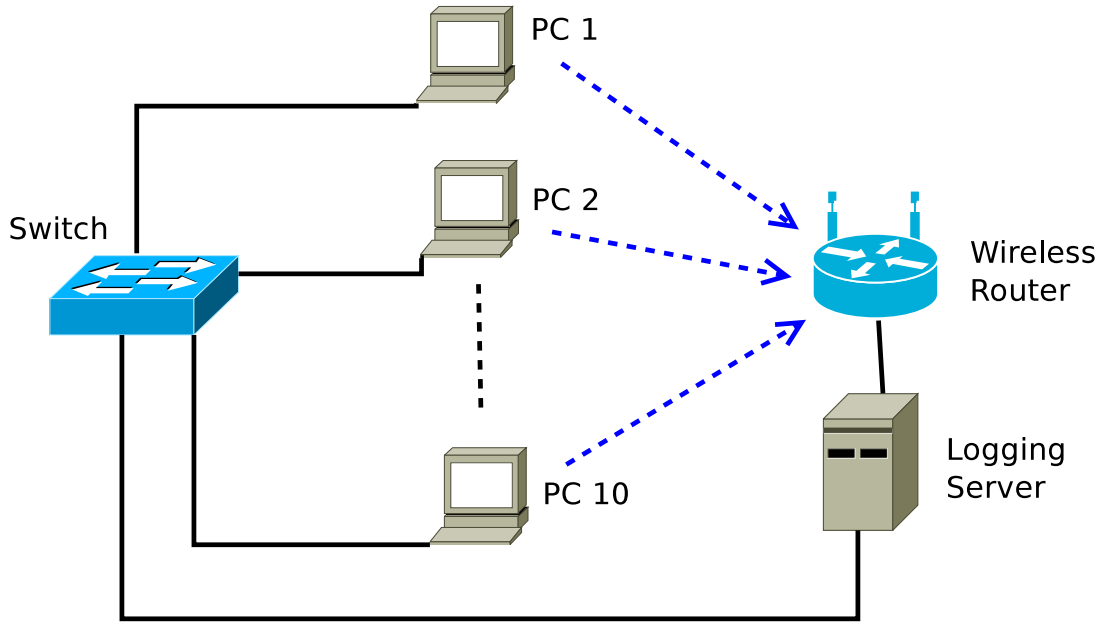
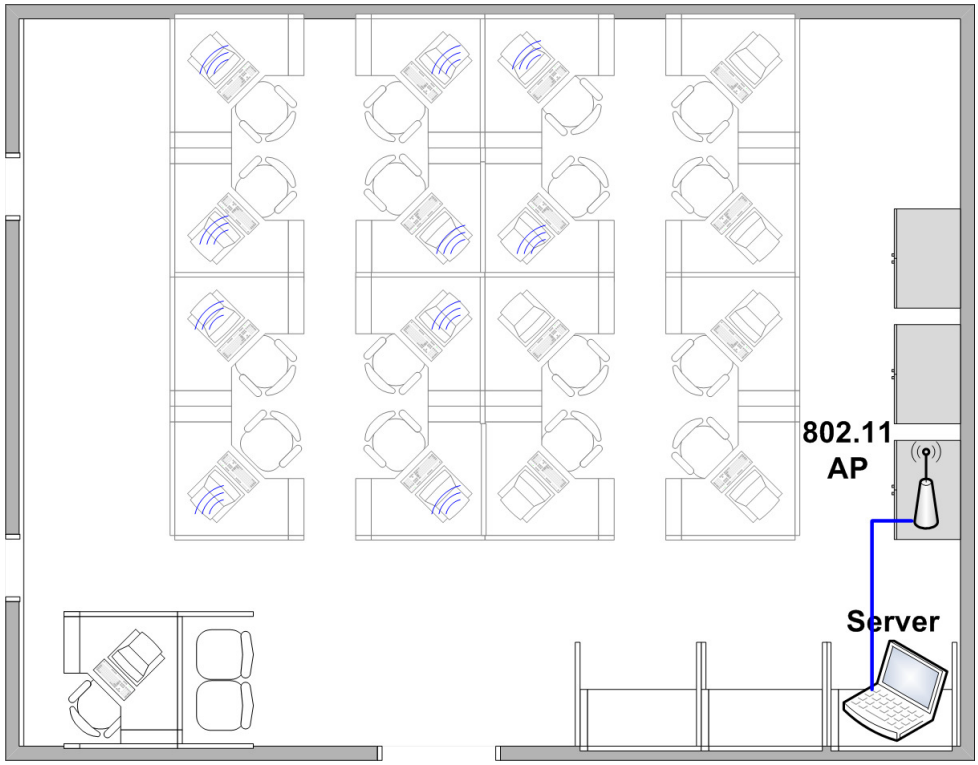


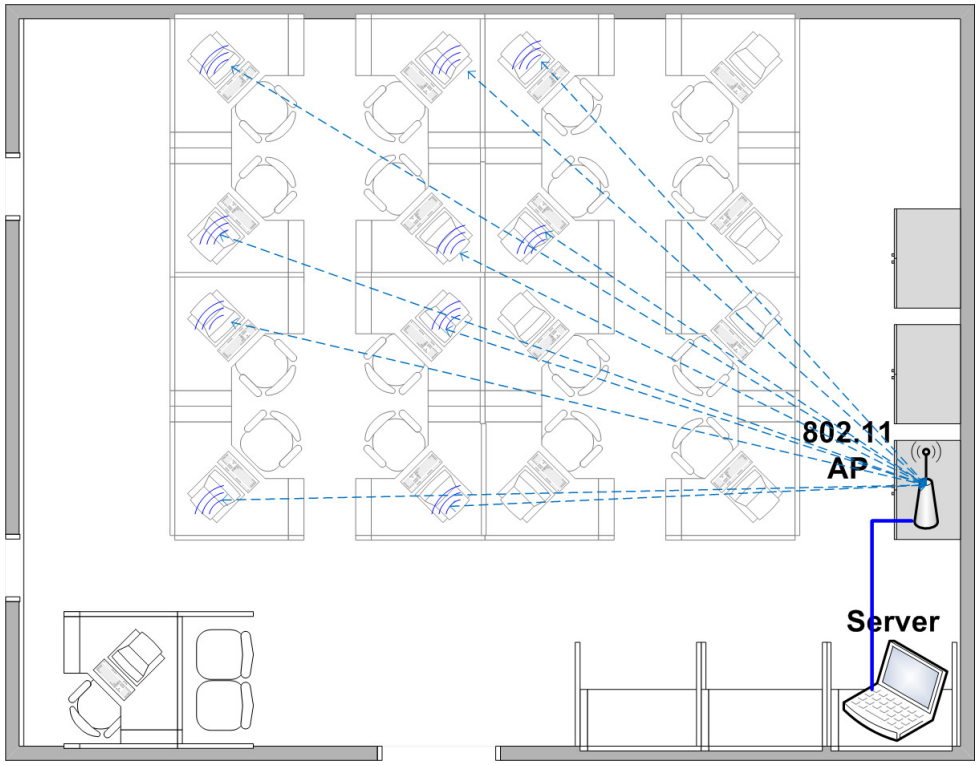
Figure 5.1: Network Connectivity Diagram for Testbed

As seen in Figure 5.1, a logging server is also connected to the same switched network of the testbed for storing the wireless packet traces in the network. This logging server is also the main control server that sends the start and stop control packets to the nodes that are a part of the wireless testbed. The wireless router that is a part of the testbed is also directly connected to the logging server by means of a wired network to ensure that the communication between the logging server and the wireless access point does not introduce any additional packets in the wireless network. The logging server also has a wireless PCI card installed for the purpose of capturing the packets on the wireless channel in promiscuous listening mode (also referred to as monitor mode).

The physical layout of the testbed is shown in Figure 5.2. This shows the layout and location of nodes in the Information Networks Laboratory [61], in Department of Electrical Engineering at Indian Institute of Technology Bombay, Mumbai, India. Figure 5.2(a) shows



(a) Physical Layout of Nodes in the Testbed



(b) Individual Flows in the Testbed

Figure 5.2: Physical Layout of the Experimental Testbed with the Indivial Nodes marked with wireless radios.

the location of the nodes that are part of the wireless testbed relative to the AP and the server. Figure 5.2(b) indicates the wireless network connectivity between the nodes and the wireless router in the testbed. As seen, all the flows in the testbed are uplink flows that send data from the IEEE 802.11 client (at the individual nodes in the testbed) to the IEEE 802.11 access point. The testbed has only infrastructure mode of communication (i.e., IEEE 802.11 access point based communication). However, since all the nodes in the testbed are close to each other and within the wireless transmission and interference range, it is safe to assume that the performance will be identical even if the flows were to be peer-to-peer. If the flows in the network were a mixture of uplink and downlink flows, then the peer-to-peer communication performance may have been different.

The physical layout figures do not explicitly show the wired network connectivity of the nodes in the testbed. However, every node that is a part of the testbed is connected to the server shown in the figure via a wired network link that is part of the switched network of the laboratory.

5.1.2 *madwifi* Driver Modifications

The driver used with the TP-Link TL-WN350GD card was *madwifi* [62]. The madwifi driver in Linux provides complete control over the wireless card to collect and maintain statistics for various operations that are important for the verification of the analytical model discussed in Sections 4.1 and 4.2. In order to validate the analytical model, we need to collect and analyze the following metrics from the wireless network; a) Probability of Collision, b) Probability of queue empty, and c) Attempt rate.

In the DCF mode of operation, where RTS-CTS-DATA-ACK packet sequence is used for transfer, the metrics are measured using the count of packets as per the below mentioned list:

1. **Probability of Collision**: Derived from
    - Count of RTS Transmissions
    - Count of RTS Timeouts
    - Count of ACK Timeouts
2. **Attempt Rate**: Derived from
    - Count of RTS Transmissions

- Session duration for the experiment

In a similar manner, in the case of Basic mode of operation, where DATA-ACK packet sequence is used for data transfer, the metrics for collision probability and attempt rate are measured using DATA packets instead of RTS. The count of variables for various metrics is summarized in Table 5.2

Table 5.2: Packet collection for measurements in the testbed

Metric	**DCF Mode**	**Basic Mode**
Probability of Collision	RTS Transmissions	Data Packet Transmissions
	RTS Timeouts	ACK Timeouts
	ACK Timeouts	
Attempt Rate	RTS Transmissions	Data Packet Transmissions
	Session duration	Session duration

In addition to the probability of collision and the attempt rate, we also derive the probability of the queue being empty in the analytical model. However, in the case of the testbed measurements, it is not possible to determine the queue length from the wireless drivers easily either directly or indirectly without having access to the firmware. Hence, for the purpose of comparisons, we only concentrate on the probability of collision and the attempt rate of packets in the wireless network. Within these two parameters, we specifically look at the collision probability with more interest as this provides with a much clearer indication of network saturation as seen in the analytical model and simulation based results from Chapter 4.

Most of the counts desired by us are directly available from the driver tools *athstats*. However, the default statistics collection accounts for every packet handled by the driver including (a) the routine MAC layer control packets to maintain active connection status with the AP and (b) probe packets to and from other APs in the vicinity. Although infrequent, these extra packets accounted for a variation in the counts desired by us, thereby affecting the accuracy of the metrics being gathered.

We also require an accurate count of the individual variables during a specific time frame (between start and stop of the data flow). This could have been achieved using difference in the counts between the two time stamps from the statistics collected. However, due to the noise introduced in the statistics by the MAC layer control and probe packets, it was essential to

modify these statistic collection routines to explicitly start and stop the counting of packets on demand.

The statistics gathered for each metrics were made available to the user-space programs via the */proc* file system [63]. The specific location in the procfs file system for the madwifi driver is */proc/net/dev/ath0/*, where textitath0 denotes the name of the wireless interface assigned by the driver to the wireless card. The list of statistics and the location of */proc* entries is given below.

1. Count of RTS Transmissions: *ast_tx_rts*,
2. Count of Data Packet Transmissions (Unique): *ast_tx_packets*
3. Count of Packet Transmissions (Retry): *tx_shortretry*, *tx_longretry*
4. Count of RTS Timeouts: *tx_errors*

In the case of *madwifi*, the statistics for RTS, retries and timeouts are available by default. The driver continues to maintain the statistics for various parameters from the moment of initialization of the wireless card using the driver. However, measurements in a controlled experiment require exact values for all the statistics for the duration of the specific experiment. In order to get an accurate count of transmitted packets for a 10 second duration of User Datagram Protocol (UDP) flow, there are two options:

- Reinitialize the wireless driver for each session of experiment,
- Force the driver to reset count for statistics on demand.

Reinitializing the driver is a simpler exercise that would have been possible without any driver modifications. However, this adds one more variable to the experiment. The statistics collected also include counts from control packets that get exchanged during the association of the node with the wireless network. In addition to this, the experiments needed varying number of nodes (from 1 to 10) to start recording statistics and start transmission of packets at the same time. Reinitializing of the wireless driver would mean re-association of all the wireless nodes in the network, hence causing loss of synchronization in the start times of flows. As a result of the complications that get introduced in the synchronization of flows due to reinitialization of the driver, it became necessary to force a reset of statistics on demand.

In the *madwifi* driver, *ath_tx_start()* is the function that is called for every packet transmission. We intoduce an extra indicator variable *collect_stats*, which enables or disables the collection of statistics within the driver. The *collect_stats* variable is initialized to a value of 1 from outside the driver at the start of the data session in an experiment and is again set to value 0 at the end of the data session. This allows fine grained control over the duration of statistic collection in the driver.

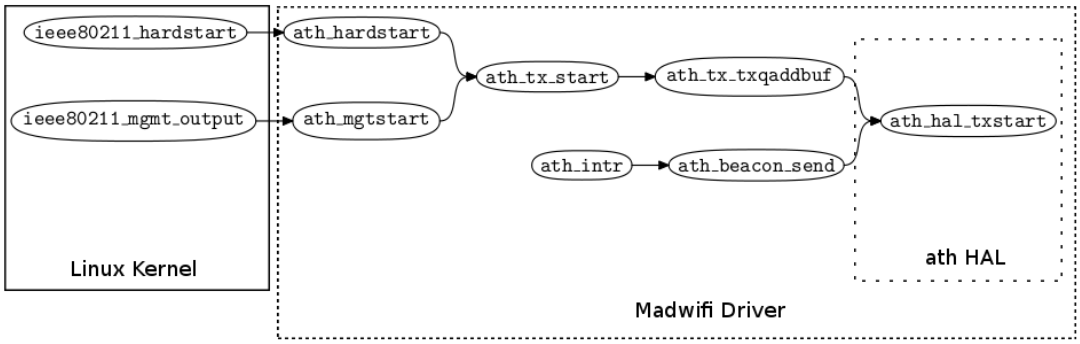


Figure 5.3: Madwifi Transmit Function Graph

Figure 5.3 shows the call flow diagram for the *madwifi* driver. The *ieee80211_hardstart* is a function call from the Linux kernel to the wireless driver *ath_hardstart* which in turn calls the transmit function *ath_tx_start*. All the statistic updates and modifications are performed in this function of the driver.

5.2 Traffic Generation

The traffic was generated using the *iperf* [64] tool. *iperf* provides the ability to generate both TCP and UDP traffic. In the case of UDP traffic, *iperf* provides the flexibility to specify the packet size, and the rate at which the packets have to be transmitted. The choice of *iperf* in lieu of other traffic generators like *udpmon* [65], *brute* [66], etc., was done because of the flexibility provided by *iperf* in extending its capabilities and the detailed throughput and delay statistics provided by *iperf*.

5.2.1 Poisson traffic generation using *iperf*

A Poisson Traffic generator for a specific packet size and data rate was implemented in *iperf*. This was done specifically to make the testbed result to be consistent with the traffic model

assumed in the analytical model. We take the desired packet size and data rate as input and determine the Poisson parameters to be used by the traffic generator. A Poisson arrival process is characterized by either of the two parameters:

- Mean λ packets per unit time,
- Mean $\frac{1}{\lambda}$ time between two packet arrivals.

The latter method utilizes the property that Poisson arrival process has Exponential inter-arrival times. Hence, we use the packet size and desired data rate to compute the average number of packets required to maintain the data rate.

$$\lambda = \frac{(dataRate \cdot 10^3)}{pktSize \cdot 8},$$

where, $dataRate$ is in terms of kbps and $pktSize$ is in terms of bytes/packet.

5.2.2 Control of Traffic Generation

The broadcast control packet contains parameters to be used for traffic generation by *iperf*, viz., packet size and data rate. The sink of all the traffic generated by all nodes is a Desktop machine connected to the uplink of the WRT54GL wireless router running an *iperf* listening server.

The Logging Server shown in Figure 5.1, also serves as the central coordinator for start and stop of experiments. A UDP client listening daemon program runs on each PC that is a part of the testbed. On receipt of a control command, the client program collects the parameters of the traffic flow to be generated and initiate the traffic generation using *iperf*. The server program running at the Logging Server constructs a special broadcast packet indicating all the nodes that are supposed to initiate the traffic flow using a bitmap pattern.

The control packet used by the server program is shown in Figure 5.4. The fields in the control packet are described in Table 5.3 As shown in the packet, the bitmap consists of 32 bits, where bit i is reserved for the i^th node in the testbed. As per the experimental setup, the bits were set to one only for those node that had to generate traffic in a particular experiment.

The action taken in response to the start and stop control packet is quite straight forward in terms of the traffic generation and Poission data flow. However, there is one additional action taken by the nodes in the testbed in response to the stop contorl packet. On receiving the stop control packet, the Nodes collect statistics from the */proc* file system and store it in a

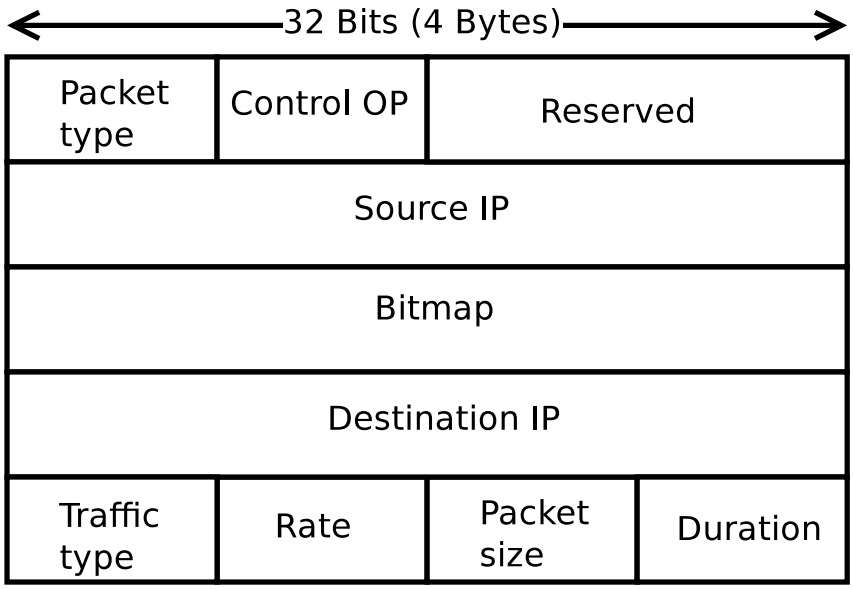


Figure 5.4: Control Packet Used for Traffic Generation

Table 5.3: Control Packet Format

Field Name	**Size (Bytes)**	**Description**
Packet Type	1	Type of Packet
Control OP	1	1 = Start Flow; 0 = Stop Flow
Reserved	2	
Source IP	4	IP Address of Control Server
Bitmap	4	If bit i is set, i^{th} node processes the packet
Destination IP	4	Destination IP Address of traffic flow
Traffic Type	1	1 = Poisson, others = reserved
Rate	1	Datarate in kbps for traffic flow
Packet Size	1	Size in bytes
Duration	1	Time in seconds

comma seperated value (CSV) file. This file is then sent to the logging server. This ensures that the logging server has a single point of storage of all experiment files for a given run of the measurement from all the nodes participating in the test in addition to the traffic logs from the wireshark capture and the statistics from the wireless router.

5.3 Validation of Analysis

In this section, we present results for the validation of the analytical results from Chapter 4. A testbed is setup as discussed in Section 5.1 with 10 Nodes, an access point and a control server.

5.3.1 Homogeneous Case

In the Homogeneous traffic case, all nodes in the network generate traffic at equal rates. For the purpose of comparison, Poisson traffic was generated with packet size of 1000 bytes. Figure 5.5 shows the comparison of testbed results with the analytical model for traffic rate of 1Mbps per node.

It can be seen that the testbed results follow the same trend as obtained in the analytical modeling. It was observed that the testbed results showed a higher degree of collision losses as compared to the analytical model. This can be attributed to various practical issues involved in the real world scenario that are not captured in the model. The analytical model is strictly modeling the MAC layer protocol and the impact of the physical layer is ignored.

The testbed is located indoors and tests run between 1am and 4am, when there is very low mobility of people in the room. Although the tests are conducted in controlled circumstances, there are significant multi-path and shadowing related artifacts that are not captured in the analytical model. However, the trend followed by the analytical model and the testbed results remains the same.

In order to explain the difference in analytical model and the testbed results more clearly, we observe one single flow of the wireless network in isolation. This is done in order to understand the impact of PHY layer conditions on a network without any other interference from competing traffic and MAC layer control actions. We performed a controlled experiment in the testbed to observe the impact of wireless channel effects on a single data traffic flow. A single flow is initiated from one of the nodes to the wireless AP. The testbed setup for the controlled experiment is shown in Figure 5.6. A data transfer is initiated for a 30 second duration. Human movement is started at 10 seconds after the start of the flow. The person moves from one end of the room to the other end in the indicated path.

As can be seen from Figure 5.7, the throughput obtained across multiple runs varies significantly. These experiment runs were conducted in a completely empty lab conditions at late hours with no other wireless traffic, hence eliminating possibility of additional interference and

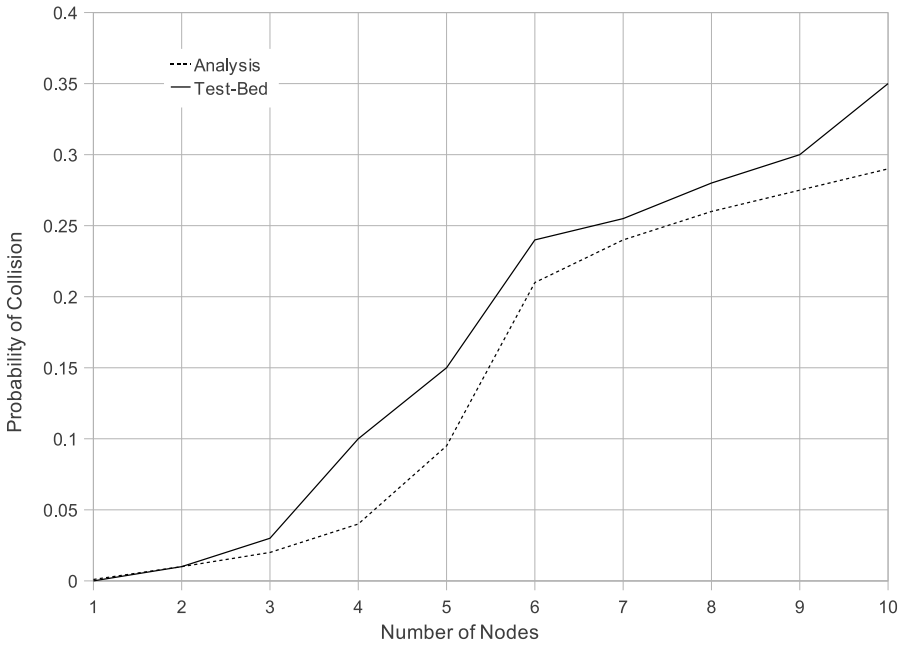


Figure 5.5: Collision Probability for 1Mbps Traffic at each node

disturbances. Run-1 shows a severe change in throughput observed when there is one person moving in the direct path between the wireless client and the access point. Run-2 shows the impact of moving a chair position in the direct path between the wireless client and the access point. It can be observed that the measured throughput remains unaffected when there is no change in the physical environment between the wireless client and the access point.

Since our analytical model does not incorporate the PHY conditions, the impact of changes due to interference, mobility of objects / people. and time varying nature of the wireless channel does not get accounted for. Hence, even with a controlled environment for the experiments, the analytical model can not capture the time varying nature of the wireless channel. It can be observed that the results obtained from the analytical model follow the same trend as measured in the testbed. The testbed results have a higher value for reported collisions. While measuring the collisions in the testbed, the reported values for collisions at the driver can not differentiate between a packet lost due to wireless error or due to collisions. Wireless errors and time varying nature of the wireless channel are aspects that are not captured by the analytical model. Hence, for the testbed, the values for collision probability are reported to be higher as compared to the analytical model.

We repeat the experiments for different arrival rates at each node in the network to find that the measurements from the experiment and the analytical model follow a similar trend and

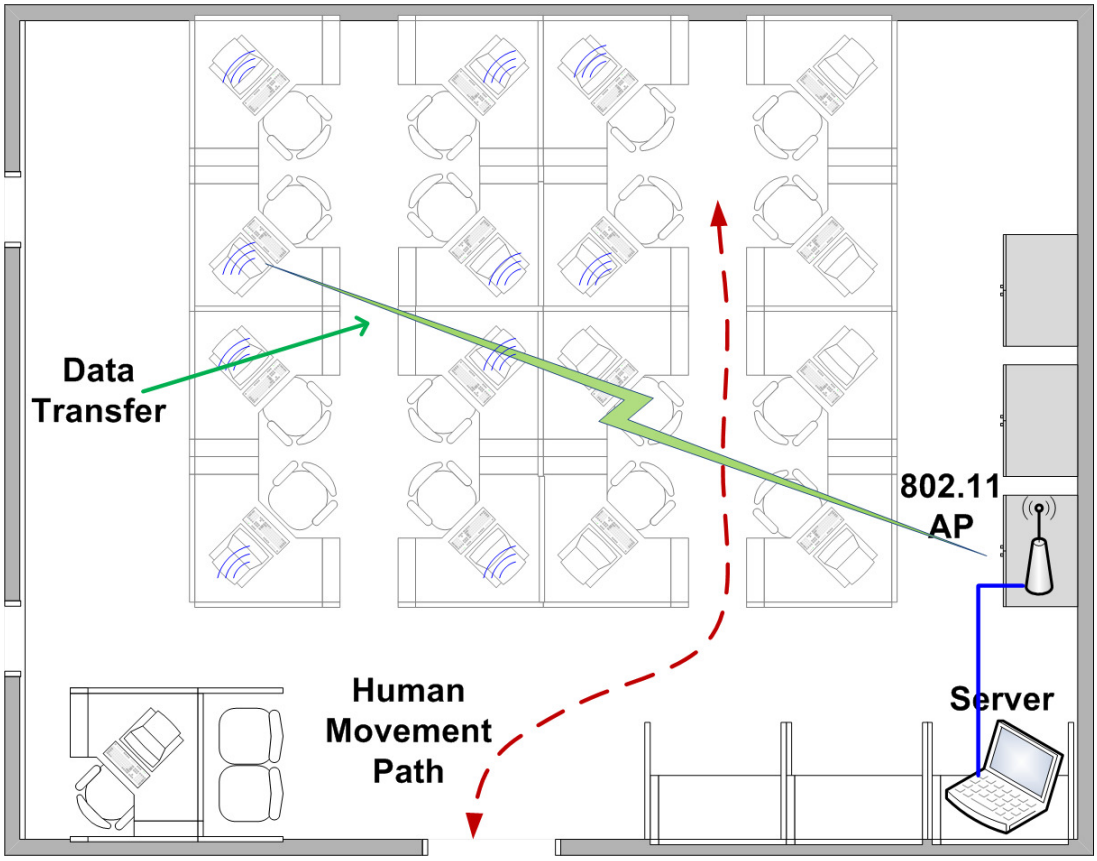


Figure 5.6: Controlled Experiment Setup with Single Data Transfer Flow

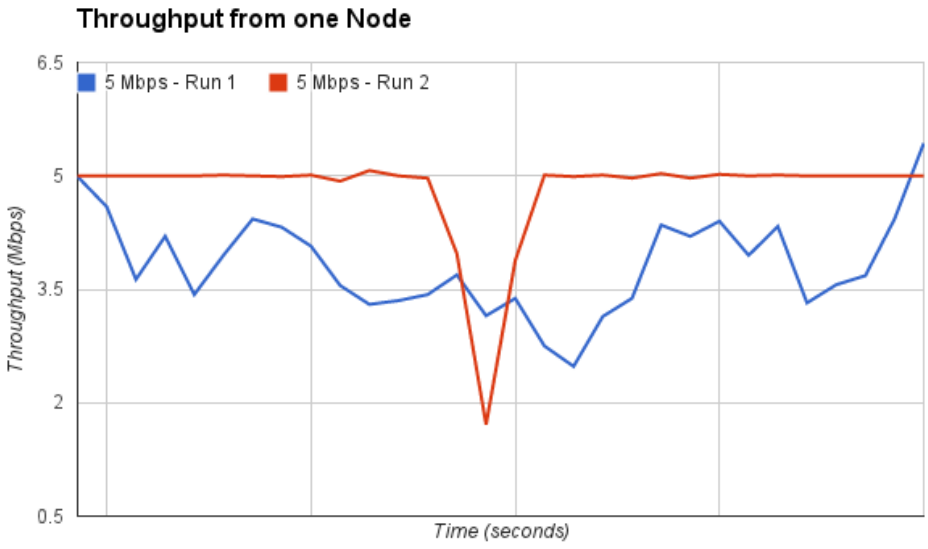


Figure 5.7: Throughput from a Single Node Transmission in the Testbed

as the number of nodes in the network increase. This same trend is observed for the collision probabilities in the experimental measurements and the analytical model.

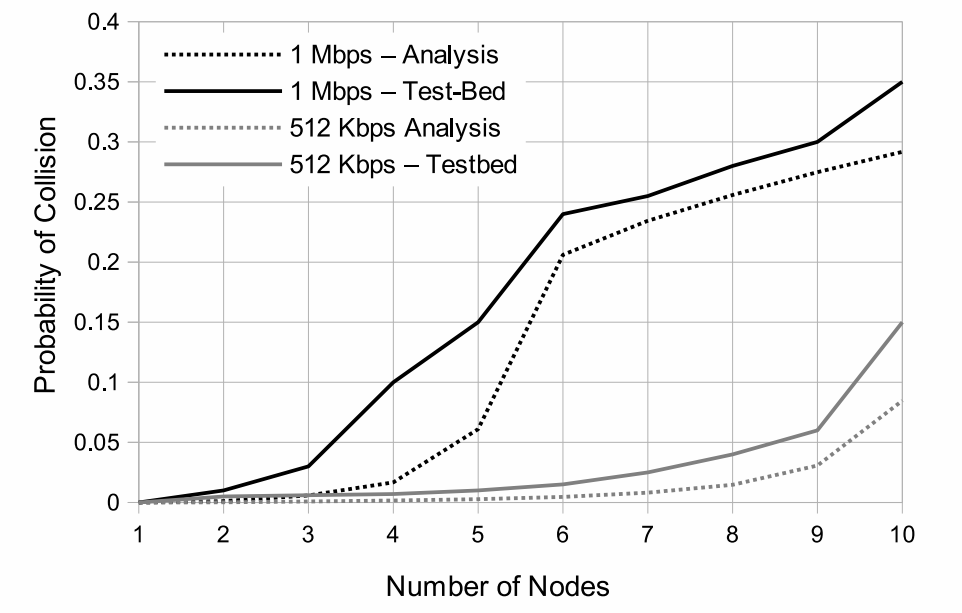
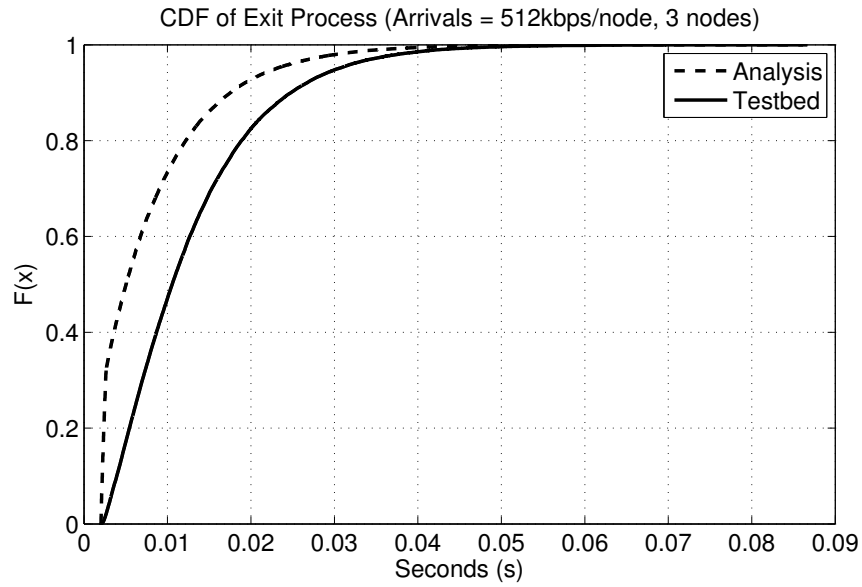


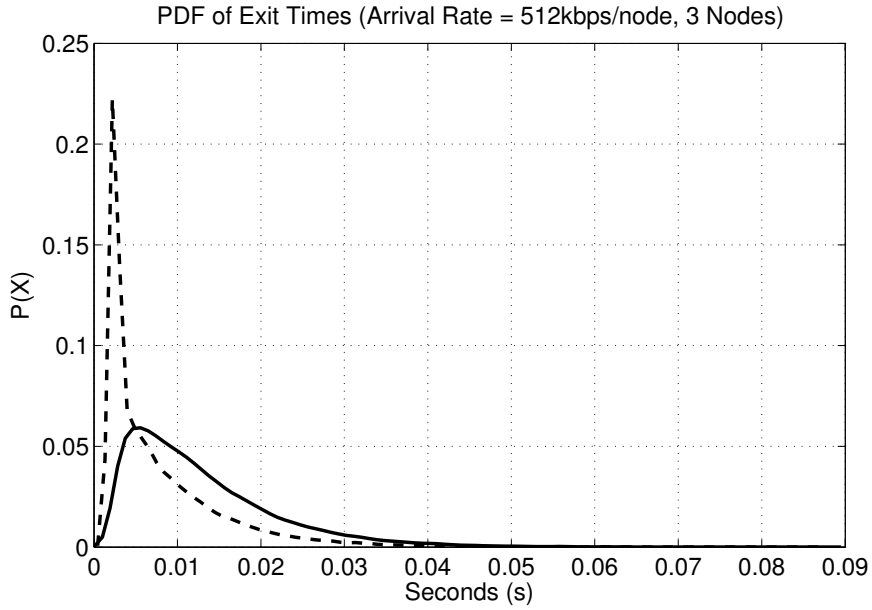
Figure 5.8: Collision Probability for varying traffic at each node

Figure 5.8 shows the comparison between the measured values for collision probability as compared to the analytical model from Section 4.1. We observe a similar trend for both 1 Mbps and 512 Kbps traffic flows at each node. As discussed, the testbed results show a higher degree of collision values due to factors such as wireless channel errors and the physical layer model that is not accounted for in the analytical model by us.

Figure 5.9 shows the Probability and Cumulative density function comparisons for the Exit Process in the homogeneous arrival case. The analytical model computes the exit times in terms of time slots in (4.6), (4.7), (4.8) and (4.10). For the purpose of plotting the graphs, we multiply each time slot by $20\,\mu s$. The Cumulative Density Function is plotted Figure 5.9(a) and the Probability Density Function is plotted in Figure 5.9(b). From the figures, it can be seen that the measurements from the tesbed are reflected well in the analytical model. As observed in the case of collision probaility, the testbed measurements are more pessimistic. The PDF and CDF plots give further insights into this discrepancy from the perspective of choice of wireless modulation scheme chosen by the packets. Since the analytical model does not incorporate the adaptive modulation scheme of the IEEE 802.11 protocol, it assumes that the packets do not use different modulation schemes each time. However, in the testbed, based on time varying nature of the channel, the packets change the modulation scheme used and hence use up slightly more amount of time during the packet transmissions.



(a) CDF of Exit Process



(b) PDF of Exit Process

Figure 5.9: Probability and Cumulative Density Function comparison of the Analytical Model as compared to Testbed with 512 Kbps arrival rate per node for 3 nodes in the network.

5.3.2 Non-Homogeneous Case

In the non-Homogeneous case, traffic generated at each node may be different. The same network is used for the experiments. We use a total of 7 nodes in the network, 4 nodes at 256 Kbps each, 2 nodes at 512 Kbps each and one node at 1 Mbps. Figure 5.10 illustrates the comparison between the analytical model and the testbed measurements.

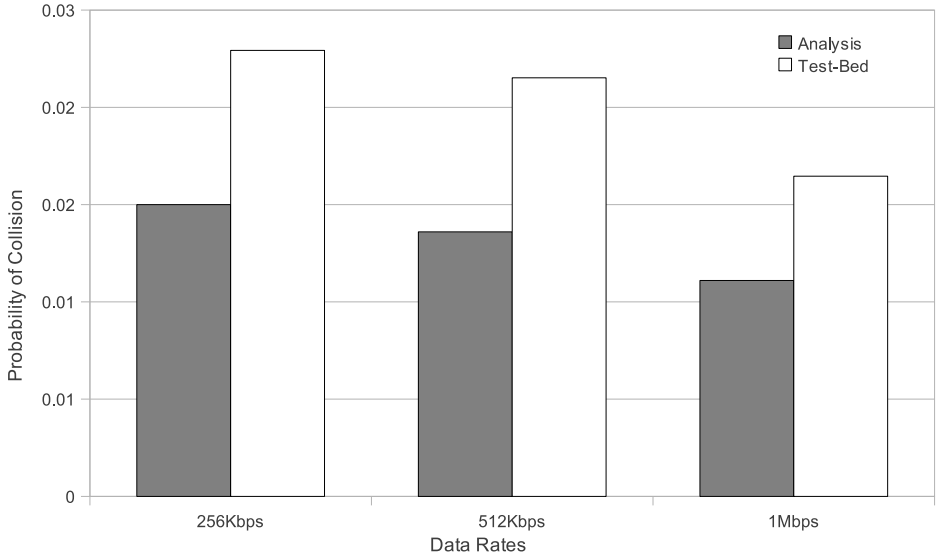


Figure 5.10: Collision Probability for Non-Homogeneous arrivals at each node

It can be seen that the trend followed by the testbed results is observed even in the analytical model. As was the case with homogenous analysis, the analytical results in non-homogeneous case are conservative with respect to computing the collision probabilities. This is because of the absence of physical layer model from the analysis.

5.4 Summary

In this chapter, we present the decision making process and and the devices used in the indoor lab testbed. We provide details of the hardware used, network topology considered and the modifications performed to the wireless drivers in order to perform measurements in the testbed. It was observed that the wireless channel is significantly affected by small changes in the environment caused. Hence, in order to validate the analytical model results that focus only on the MAC layer issues, the testbed experiments had to be performed at idle hours so that temporal variations in the wireless channel are minimized. We also demonstrate that the analytical model for both homogeneous and non-homogeneous case follow the trend as measured from testbed experiments. A close match is not observed between the testbed and analytical model due to the wireless channel variations that are not captred by the analytical model.

Chapter 6

Characterizing the Performance of Backhaul Network

An IEEE 802.11 based access network can provide network connectivity that spans a few hundred meters [11]. In order to ensure connectivity to the IEEE 802.11 based access network (refer Section 1.2.1), in the context of an Indian Rural scenario as discussed in Chapter 1, it becomes essential to link the access networks, that serve the purpose of a local area network (LAN) to the Internet using wide area network (WAN) links. In the context of this chapter a fixed wireless deployment of IEEE 802.16 is considered[11]

In this chapter, we consider a basic IEEE 802.16 network deployment in the backhaul network. The IEEE 802.11 based access network serves as the traffic load that feeds data into the IEEE 802.16 backhaul network. We formulate an analytical model to analyze the queuing behavior in a hybrid network topology with access network traffic originating in the IEEE 802.11 cell with a backhaul network provided by IEEE 802.16.

The departure process at the IEEE 802.16 Subscriber Station (SS) in the backhaul network is dependent on the scheduling algorithm being used in the backhaul network by the IEEE 802.16 Base Station (BS) and the traffic arrivals at the individual IEEE 802.16 SS. In this chapter, we consider a round robin scheduling algorithm at the IEEE 802.16 BS. This assumption is

[11]Even though we consider a fixed IEEE 802.16 based network for the backhaul in this chapter, the choice of backhaul network technology is not limited to IEEE 802.16 alone. There could be many other options including a) Long distance IEEE 802.11 links, b) TV White Space radios with point-to-point, point-to-multipoint and mesh topologies, c) 4G technologies like LTE and LTE-Advanced in the unlicensed and TV White Space bands and d) Proprietary radios like Carlson Wireless, Adaptram etc.

made in order to reflect the sparce nature of deployment of the backhaul network. For arrivals at the IEEE 802.16 SS, we use the the departure process statistics from the IEEE 802.11 cell as derived in Chapter 4.

As a result of the analysis, we determine the average time spent by the access network packets in the wait queue at the edge of the backhaul network. We also determine the utilization and average waiting times in the IEEE 802.16 backhaul network in order to understand the stability of queues.

In this chapter, we discuss the system model in Section 6.1. The analysis for round-robin scheduling by the BS is discussed in Section 6.2. Comparison between the analytical model and simulations is presented in Section 6.3.

6.1 System Model

Consider an IEEE 802.16 cell, where the IEEE 802.16 cell is defined in the same manner as the IEEE 802.11 cell. An IEEE 802.16 BS is connected to multiple IEEE 802.16 SSs which in-turn are connected to the IEEE 802.11 cells. This creates a hierarchical network of hybrid nodes, both IEEE 802.11 and IEEE 802.16. The link between the IEEE 802.16 BS and SS may be cover a distance of a few hundred meters to provide connectivity to the IEEE 802.11 access networks.

We consider a collocated IEEE 802.16 Subscriber Station (SS) along with the IEEE 802.11 Access Point (AP). The traffic in the network is generated at the IEEE 802.11 clients in the network. The individual IEEE 802.11 clients are connected to the IEEE 802.11 AP. The AP is the aggregation node for the traffic generated in the network discussed in Chapter 4.

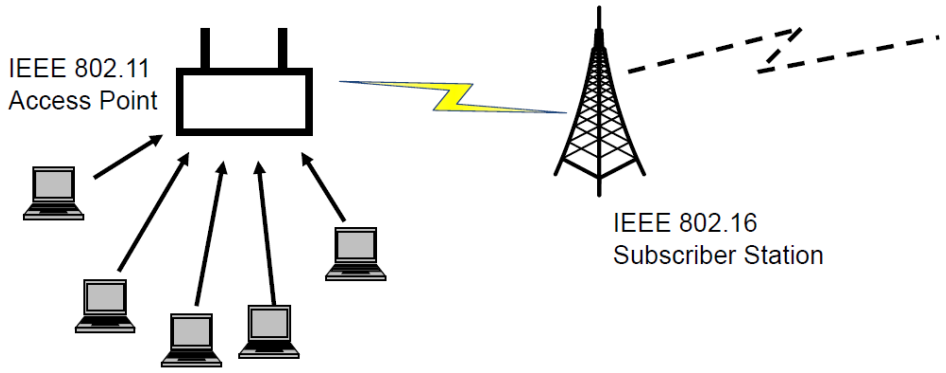


Figure 6.1: Typical Network Layout with Co-located IEEE 802.11 Access Point and IEEE 802.16 SS.

A typical network layout is shown in Figure 6.1. It is also possible to connect more than one IEEE 802.11 cell to the IEEE 802.16 SS. The IEEE 802.11 AP and the IEEE 802.16 SS are connected using a high capacity link. It is assumed that this link connecting the IEEE 802.11 AP and IEEE 802.16 SS is not the bottleneck in the communications. This is a reasonable assumption considering the fact that the AP to SS link is a dedicated point-to-point short distance wired link. There is no contention for the resources in the link between the AP and SS.

In addition to these conditions, the uplink communication from the IEEE 802.16 SS to the IEEE 802.16 BS is controlled by the scheduling constraints of the BS, the wireless channel and the load generated by the other SS connected to the IEEE 802.16 network. The outgoing packets from an IEEE 802.11 cell, as discussed in Section 4.1.2, are fed to the Subscriber Station (SS) of the IEEE 802.16 network. The SS, in turn, transmits the packets to the BS according to the time-slots assigned to it by the IEEE 802.16 Base Station (BS). The BS decides on the schedule for transmissions by the SS depending on the load and the demand generated by each SS connected to it.

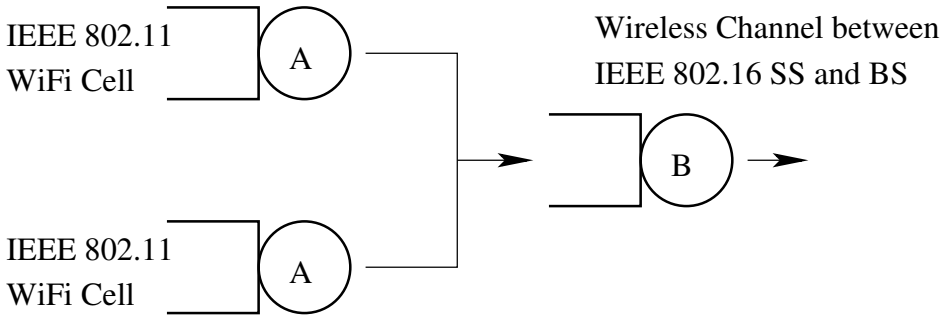


Figure 6.2: Queueing Network Model for IEEE 802.16 Backhaul Network.

We model the wireless network as a network of queues as shown in Figure 6.2. The queues labeled 'A' represent the IEEE 802.11 WiFi cell. The packets of a given cell are aggregated and forwarded by its IEEE 802.11 Access Point (AP) to the IEEE 802.16 SS. This is represented by the queue A in the figure. We adopt a similar methodology as discussed in the case of IEEE 802.11 cell to model the service time of the IEEE 802.16 network. We consider the wireless channel between the IEEE 802.16 SS and the IEEE 802.16 BS as the server of the queue labeled 'B'. The traffic from multiple IEEE 802.11 APs is multiplexed at the MAC layer of the IEEE 802.16 SS. The scheduling algorithm at the BS determines the quantum of resources alloted to each SS for transmission and hence the service time of the queue B.

6.2 Queueing Analysis of Homogeneous Case

For the purpose of this analysis, we consider the collocated IEEE 802.11 cell to be the Homogeneous Arrival Case as discussed in Section 4.1 and a round-robin scheduling at the IEEE 802.16 BS. We assume that all the SS connected to the BS have identical load, i.e., equal number of IEEE 802.11 cells connected to the SS.

6.2.1 Arrivals to the SS

In the simple case where the number of IEEE 802.11 cells connected to the IEEE 802.16 SS is one, the inter-exit time derived in Section 4.1.4.1 becomes the inter-arrival time for the arrival process to queue B in Figure 6.2. The time between two departures for the IEEE 802.11 exit packets (time between two arrivals in the current context) is given by (4.6), (4.7), (4.8), and (4.10). From the analysis of the inter-exit time distribution of the IEEE 802.11 cell, it can be seen that the departure process is Non-Markovian. Hence, for the arrival process to the queue B is a Generic Arrival process.

Consider k IEEE 802.11 cells connected to the IEEE 802.16 SS in the network. In this case, the inter-arrival time for packets at the SS is the aggregate arrival at all the IEEE 802.11 cells combined. In order to determine this combined arrival process from more than one IEEE 802.11 cell, consider the mean inter-exit time from j^{th} IEEE 802.11 cell, connected to the SS, to be as denoted by $\frac{1}{\lambda_j}$. Hence, the arrival rate to the SS from the j^{th} IEEE 802.11 cell is λ_j.

Each IEEE 802.11 cell operates independently of each other, hence, the random variables denoting the inter-exit times of each IEEE 802.11 cell can be treated as an independent. In the condition that the IEEE 802.11 cells have the exact same parameters for number of client nodes and IEEE 802.11 backoff parameters, the inter-exit time random variables from multiple cells can be treated as independent and identical.

From the linearity property of expectation of independent random variables, we have

$$E[X + Y] = E[X] + E[Y],$$

where, X and Y are two discrete and independent random variables.

The inter-arrival time for the arrival process to queue B in Figure 6.2 is the sum of k random variables that represent the k different independent random variables for inter-exit times from IEEE 802.11 cells. As determined in Section 4.1, the time between two departures for the

IEEE 802.11 exit packets is given by (4.6), (4.7), (4.8), and (4.10). Being non-markovian in nature individually, the arrivals from each cell can be treated as a generic arrival process. So, the mean of aggregate load at each SS in terms of the arrival rate can be computed as

$$\lambda_{SS} = \sum_{j=1}^{k} \frac{1}{\mu_j}, \tag{6.1}$$

where μ_j is the departure rate for j^{th} IEEE 802.11 cell connected to the SS. Upto k IEEE 802.11 cells can be connected to the SS and the aggregate arrival rate at the SS is the summation of the arrival rates from each cell.

We have the Probability Density Function (PDF) of the inter-exit times from an IEEE 802.11 cell from (4.6).

$$\begin{aligned} P(X = x) = q_0^n P(X = x|A) \\ + (1 - q_0^n) P(X = x|A^c) \end{aligned} \tag{6.2}$$

, where X denotes the number of slots, A is the probability that all nodes in the IEEE 802.11 cell have an empty queue, A^c is the probability of having at-least one backlogged node in the IEEE 802.11 cell, and q_0 the probability that there a given node among the n nodes in the IEEE 802.11 cell has an empty queue.

From (6.1) and (6.2),

$$\mu_j = \text{IEEE 802.11 slot length} \cdot E[X_j], \tag{6.3}$$

where, the mean inter-exit time for the j^{th} IEEE 802.11 cell is the mean number of slots between two departures and the IEEE 802.11 slot length is the time duration for each slot as discussed in A.3.

In the topology being considered, there may be more than one SS connected to the IEEE 802.16 BS. Consider the i^{th} SS connected to the BS to be denoted as SS_i. We denote the arrival rate at the individual SS as λ_{SS_i}. The BS receives indication of the aggregate load at each SS in terms of the average arrival rate computed as shown in (6.1).

6.2.2 Departures from the SS

The IEEE 802.16 BS can have multiple SS connected to it. In this particular use-case of the network, the IEEE 802.16 SS and the BS form a part of the backhaul connectivity for the IEEE 802.11 access network.

The IEEE 802.16 standard [12], specifies various classes of service. In our case, we consider a round-robin scheduling scheme at the IEEE 802.16 BS with fixed amount of bandwidth reserved for each SS in the network. The BS provisions the resources allocated to SS in a periodic manner using the round-robin schedule. The number of time slots assigned depends on the amount of load indicated to the BS in terms of aggregate arrival rate at the SS.

6.2.3 Waiting Time and Utilization

As discussed in Section 6.2.1, the arrivals to the IEEE 802.16 SS follow a generic distribution with independent arrivals from the IEEE 802.11 AP as computed in (6.1). The departures from the IEEE 802.16 SS take a deterministic time as a result of the round-robin scheduling by the BS. Based on this, we can model the SS queue as a GI/D/1 queue, which indicates generic arrivals and deterministic departures with one server. The waiting time for a GI/D/1 queues can be computed as a special case of the GI/M/1 queues. Using the Kulbatzki approximation of the Allen-Cunneen formula [67], we have

$$\overline{W} \approx \frac{\rho_{SS}/\mu_{SS}}{1-\rho_{SS}} \cdot \frac{C_A^{f(C_A,C_B,\rho_{SS})} + C_B^2}{2}, \tag{6.4}$$

where,

$$\begin{aligned} C_A &= \text{Co-efficient of variation of Arrivals,} \\ C_B &= \text{Co-efficient of variation of Departures,} \\ \rho_{SS} &= \frac{\lambda_{SS}}{\mu_{SS}}, \\ \lambda_{SS} &= \text{Arrival Rate at SS,} \\ \mu_{SS} &= \text{Departure Rate of SS,} \end{aligned}$$

and

$$f(C_A, C_B, \rho_{SS}) = \begin{cases} 1, & C_A \in \{0,1\}, \\ [\rho_{SS}(14.1C_A - 5.9) + (-13.7C_A + 4.1)]C_B^2 & \\ +[\rho_{SS}(-59.7C_A + 21.1) + (54.9C_A - 16.3)]C_B & \\ +[\rho_{SS}(C_A - 4.5) + (-1.5C_A + 6.55)], & 0 \leq C_A, \leq 1 \\ -0.75\rho_{SS} + 2.775 & C_A > 1. \end{cases} \tag{6.5}$$

The coefficient of variation of a random variable is given by the formula

$$C = \frac{\sigma}{\mu},$$

where, C is the coefficient of variation, σ is the standard deviation and μ is the mean value for the random variable.

In the particular case that is under consideration, $C_B = 1$ as the departure process uses a deterministic time. Also, from the observed values of the analytical evaluation in Section 4.1.4.2, C_A is always in the range 0 to 1. Hence, when $C_B = 1$, (6.5) can be rewritten as

$$\begin{aligned} f(C_A, C_B, \rho_{SS}) &= [\rho_{SS}(14.1C_A - 5.9) + (-13.7C_A + 4.1)]C_B^2 \\ &\quad +[\rho_{SS}(-59.7C_A + 21.1) + (54.9C_A - 16.3)]C_B \\ &\quad +[\rho_{SS}(C_A - 4.5) + (-1.5C_A + 6.55)] \\ &= \rho_{SS}[C_A(14.1 - 59.7 + 1) + (-5.9 + 21.1 - 4.5)] \\ &\quad +[C_A(-13.7 + 54.9 - 1.5) + (4.1 - 16.4 + 6.55)] \\ &= \rho_{SS}[-44.6C_A + 10.7] + [39.7C_A - 5.75] \end{aligned} \tag{6.6}$$

Also, (6.4) can be rewritten as

$$\overline{W} \approx \frac{\rho_{SS}/\mu_{SS}}{1 - \rho_{SS}} \cdot \frac{C_A^{f(C_A, C_B, \rho_{SS})} + 1}{2}. \tag{6.7}$$

Once the waiting time for packets in a queue is obtained using (6.7), the queue length at the SS can be computed easily using Little's law,

$$Q_{length} = \lambda_{SS} \cdot \overline{W}. \tag{6.8}$$

Utilization

The Utilization of the link between the SS and BS indicates the stability of the queues at the SS. A value of utilization (ρ_{SS}) less than 1 is desirable to maintain stability of the queues. If the utilization is more than one 1, it indicates that the arrival rate aht the SS is larger than the rate of departure of packets from the SS, which leads to the queues getting full and packets being dropped at the SS, which is undesirable.

Given the fixed round-robin schedule of the IEEE 802.16 links, μ_{SS} is deterministic. The arrivals to the SS queue can be computed from the number of IEEE 802.11 cells connected to it from 6.1.

6.3 Evaluation of the Model

We simulate the hybrid network with IEEE 802.11 based access network and an IEEE 802.16 based backhaul network in QualNet simulator [49]. In order to speed up the simulations, we use the detailed protocol implementation only for the IEEE 802.16 for the backhaul network. The access network is simulated using an implementation of our analytical model derived in Chapter 4. The analytical model from (4.6), (4.7), (4.8) and (4.10) is implemented as a traffic generator module in QualNet simulator. The implementation in QualNet allows a user to configure the number of nodes and the arrival rate at each node in the network. This traffic generator module allows us to model a single IEEE 802.11 cell with one AP and multiple client devices. The time between two packets generated from this module accurately represents the behavior of packets leaving an IEEE 802.11 cell as seen in Chapter 5. The use of this module allows us to significantly reduce the number of nodes to be simulated in a hybrid network and hence resulting in faster simulation.

This implementation of IEEE 802.11 traffic generator in QualNet allows us to configure a hybrid topology using just IEEE 802.16 BS and IEEE 802.16 SS devices. The traffic from IEEE 802.16 SS to the IEEE 802.16 BS follows the IEEE 802.11 traffic model. The accuracy of the IEEE 802.11 analysis has been already established in Section 4.1.3.4 and 4.1.4.2, so such a configuration in QualNet simulations can be treated as equivalent to a detailed configuration with the entire hybrid network topology.

For the backhaul network, an IEEE 802.16 BS allows several classes of service depending on different Quality of Service (QoS) categories. In our case with a fixed round robin schedule, the best match is the Uninterrupted Grant Service (UGS) class of service with a dedicated reservation of bandwidth resources for each SS as per the rates demanded at the beginning of the schedule. In our implementation in QualNet, the aggregate arrival rate that is fed to the SS from the IEEE 802.11 model is already available before the start of the simulation and can be used as an estimate for the average load at the SS and can be used as the bandwidth request parameter in UGS by the SS.

The individual SS are placed within a 500 meters radius of the IEEE 802.16 BS. The IEEE 802.11 APs are collocated along with the SS. Since we use an IEEE 802.11 traffic model to emulate an IEEE 802.11 wireless cell, we do not need to decide placement of individual IEEE 802.11 client nodes in the simulation topology. In order to emulate the IEEE 802.11 cell, the following parameters are used in the IEEE 802.11 traffic model:

Table 6.1: Parameters used for IEEE 802.11 cell traffic model

Parameters	**Values**
Number of Clients per AP	1 to 30
Cell size	250 x 250 meters
Packet size	1500 bytes
IEEE 802.11 variant	IEEE 802.11g
Long retry limit	7
Short retry limit	4
RTS Threshold	0 Bytes

The main focus for studying the hybrid network topology is to determine the impact of the IEEE 802.11 traffic on the backhaul network.

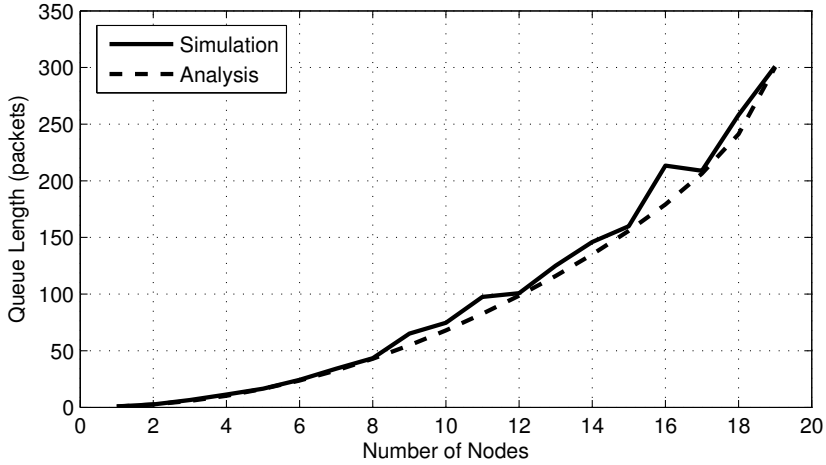
6.3.1 Simulation Parameters

The simulation parameters used in the experiments are as follows:

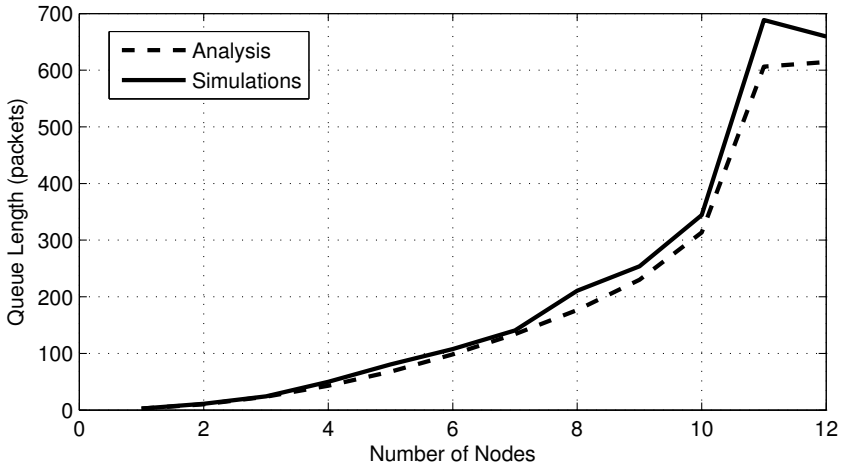
Table 6.2: Parameters used in Simulations and for the Analytical Model

Parameters	**Values**
Number of WiFi cells per SS	1
Arrival rate at each node	256 kbps to 1 Mbps
Simulation time	300s

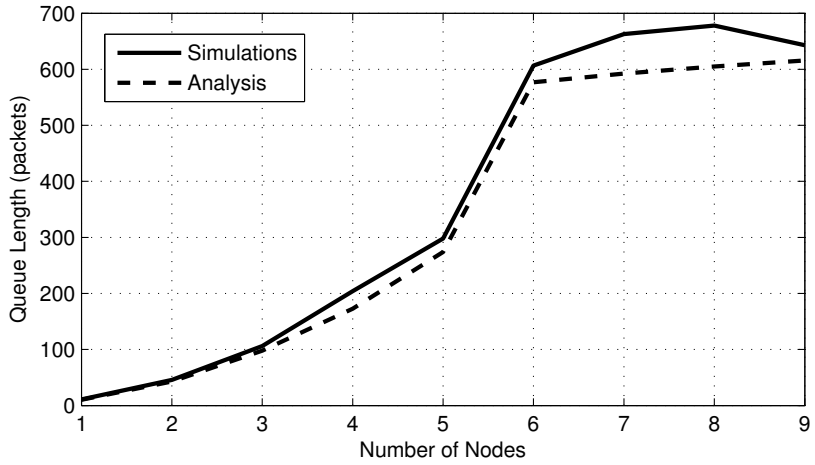
We vary the number of WiFi clients connected to a single IEEE 802.11 / IEEE 802.16 cell by adding additional 802.11 traffic flows. For the simulation, the IEEE 802.11 traffic generator model is configured appropriately to vary the number of nodes in the IEEE 802.11 cell and the data rate for arrivals at each node in the cell. Each IEEE 802.16 SS has exactly one IEEE 802.11 AP connected via a wired Ethernet link. This results in the network topology where every IEEE 802.16 SS represents a single IEEE 802.11 cell in the network.



(a) Queue Length v/s Number of Nodes in IEEE 802.11 cell



(b) Queue Length v/s Number of Nodes in IEEE 802.11 cell



(c) Queue Length v/s Number of Nodes in IEEE 802.11 cell

Figure 6.3: Each figure represents the network with a single IEEE 802.11 cell with varying arrival rates: (a) 256 kbps; (b) 512 kbps; and (c) 1 Mbps arrival rate per Node;

6.3.2 Discussion

Figures 6.3 and 6.4 show the comparision between the analytical mode and the simulation results in QualNet for different configurations of the hybird IEEE 802.11, IEEE 802.16 network. The hybrid network under consideration has 5 IEEE 802.16 SS connected to the IEEE 802.16 BS. Each IEEE 802.16 SS is connected to an IEEE 802.11 AP using a wired Ethernet link. The individual IEEE 802.11 AP serves several wireless clients with varying arrival rates. The horizontal axis in the graphs, represent the number of nodes (clients) connected to the IEEE 802.11 AP in the network. Every plot represents an averaged result across all the 5 different IEEE 802.11 AP - IEEE 802.16 SS cell.

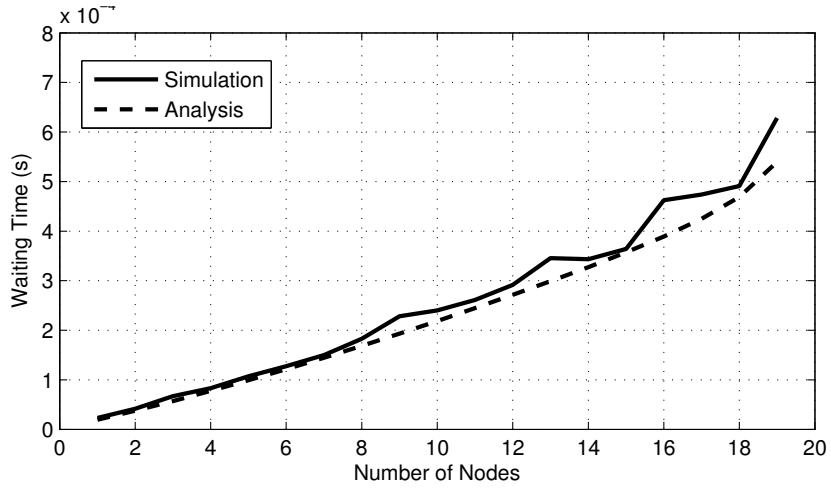
From Figures 6.3(a), 6.3(b), and 6.3(c) it can be seen that, as the number of nodes increases in the IEEE 802.11 cell, the average queue length build up at the SS increases. In the case of 512 kbps arrival rate, it can be seen from Figure 6.3(b) that the hybrid network saturates when approximately 11 IEEE 802.11 nodes are connected to the IEEE 802.11 AP / IEEE 802.16 SS. This results in a total offered load of approximately 5.5 Mbps from the IEEE 802.11 AP. This also indicates that the saturation in the network is heavily dominated by the IEEE 802.11 network capacity.

Depending on the kind of traffic and applications to be used by the end users, these results can be used to arrive at an estimate of the number of wireless clients that can be supported in the network without violating delay or queue length constraints.

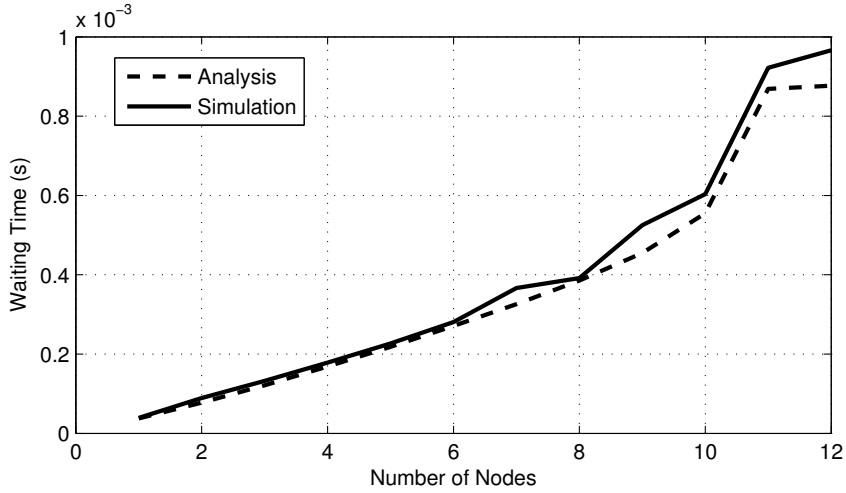
It can be seen that the IEEE 802.11 Cell reaches a saturation point in the case of 1 Mbps arrival rates per Node as seen in 6.3(c) at around 5 or 6 nodes in the cell. Even in this case, the approximate offered load is 5.5 Mbps at the IEEE 802.11 AP / IEEE 802.16 SS.

In case of both 512 kbps and 1 Mbps arrival rates at individual IEEE 802.11 nodes, the network saturation is reached at approximately 600 packets in the queue as seen in Figures 6.3(b) and 6.3(c). At packet size of 1500 bytes, this results in a queue length of approximately 900 kbytes. The similarity in both 512 kbps and 1 Mbps flows also indicate the dominance of IEEE 802.11 access network contributing heavily to the saturation behavior in the hybrid network.

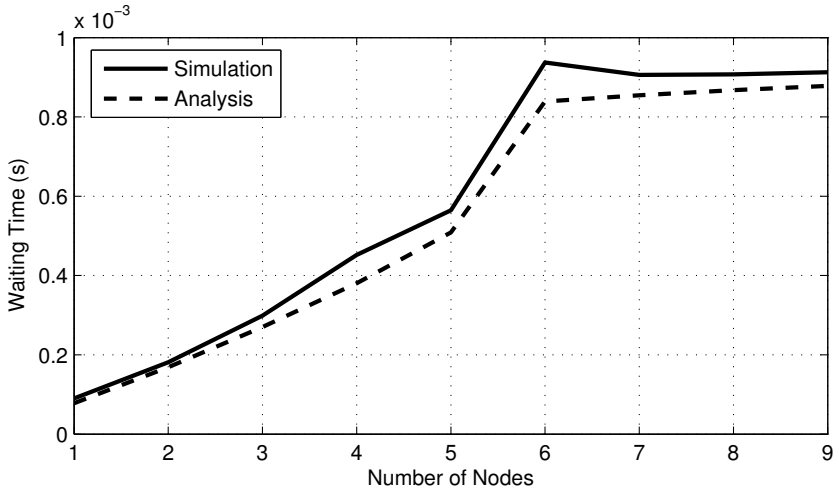
For the waiting time in the network, a similar behavior is observed from Figures 6.4(a), 6.4(b) and 6.4(c). The average waiting time reaches a saturation point at around 80 ms for 512 kbps and 1 Mbps arrival rate at the IEEE 802.11 nodes in the network. The network supports approximately 10 nodes in the case of 512 kbps arriaval rate; and approximately 5 nodes and



(a) Wait Time v/s Number of Nodes in IEEE 802.11 cell



(b) Wait Time v/s Number of Nodes in IEEE 802.11 cell



(c) Wait Time v/s Number of Nodes in IEEE 802.11 cell

Figure 6.4: Each figure represents the network with a single IEEE 802.11 cell with varying arrival rates: (a) 256 kbps; (b) 512 kbps; and (c) 1 Mbps arrival rate per Node;

in the case of 1 Mbps arrival rate. This is similar to the observation from queue length at IEEE 802.16 SS in the network.

In order to put the results from the hybrid network in context of a real world deployment, if the user applications demand a 50 ms delay constraint, the network can only support upto 8 nodes in the IEEE 802.11 cell, where each node has a 512 kbps arrival rate as seen from Figure 6.4(b).

6.4 Summary

In this chapter, we have presented the queuing network model for a hierarchical IEEE 802.11, IEEE 802.16 network. We have also implemented and used the IEEE 802.11 traffic generation module to simplify and speed up the simulations for such a hierarchical network. The round-robin scheduling in the IEEE 802.16 backhaul network along with IEEE 802.11 arrival rates is modeled as a GI/D/1 queue and the average waiting times and queue lengths are determined. In the sparse deployment scenarios considered by us when the access network is lightly loaded, we observe that the backhaul network may be able to sustain the load. We have also validated the analytical model at the IEEE 802.16 SS by comparing the results with QualNet simulations. Even though we consider IEEE 802.16 as the backhaul network technology, the results in this chapter are largely valid as long as the scheduling algorithm assumptions remain the same.

Chapter 7

Co-Existence of WiFi and WiMAX

In this chapter, we discuss the problem of coexistence of WiFi and 4th Generation (4G) technologies due to adjacent channel interference. The existing literature has many solutions to address the problem of shared channel coexistence and adjacent channel coexistence on multi-radio platforms as outlined in Section 2.2. Results for non-collocated coexistence in adjacent channels in wireless remain very scattered and few as seen in Section 2.2. Radio devices operating on Broadband Wireless Access (BWA) 4G wireless technologies like IEEE 802.16, Worldwide Interoperability for Microwave Access (WiMAX), and 3rd Generation Partnership Project (3GPP) Long Term Evolution-Advanced (LTE-A) require very low noise floor. BWA spectrum allocations in 2.3 GHz and 2.5GHz have resulted in these networks to be very close to 2.4 GHz licence-free band used by WiFi. We show, with measurements on our testbed and from existing results [68] [69], that the low-cost filters on WiFi devices are not very effective in controlling the out-of-band emissions to satisfy the low noise floor requirements of -114 dBm required by 4G technologies like WiMAX and LTE-A. We propose schemes to mitigate the problem of adjacent channel interference by a time sharing mechanism across technologies by protecting packet receptions on both IEEE 802.11 and the IEEE 802.16 side. We demonstrate the effectiveness of our scheme to protect WiMAX packets using a testbed. We also show that there is very limited adverse impact, due to the use of our scheme, on the system throughput of the non-collocated WiFi network operating in the adjacent channel.

In this chapter, we consider WiMAX as the 4G technology that operates on the adjacent channel to WiFi. We propose a solution to mitigate interference from adjacent channels in non-collocated coexistence. The proposed scheme can be extended for other technologies like LTE and LTE-Advanced.

Wireless broadband networks aim to provide very high data rates to users at much higher distances as compared to indoor WiFi networks. Significant amount of research effort is directed towards optimizing the spectrum efficiency of wireless technologies to extract the maximum possible throughput from the minimum possible spectrum. However, spectrum is a limited natural resource and many wireless technologies are being packed close to each other in adjacent channel bands. The allocations for 4G technologies such as WiMAX and LTE in India include the 2.3 GHz and 2.5 GHz bands [70] . These frequencies are adjacent to the unlicensed 2.4 GHz band and a cause of concern that we explore in this chapter.

The 2.4 GHz license-free band is very densely populated with IEEE 802.11 WiFi and Bluetooth devices. IEEE 802.11 a/b/g devices are known to cause interference in both overlapping channels and adjacent channels [71]. Any signal transmitted outside the 20 MHz channel bandwidth of a WiFi channel is an out-of-band signal. The interference in adjacent channels is largely due to poor out-of-band signal rejection of IEEE 802.11. This raises a concern that devices from different technologies may not coexist gracefully even when they do not share the same spectrum. We refer to this situation as non-collocated coexistence in adjacent channels.

With the recent advances in highly portable gadgets like tablets, netbooks, ultrabooks and smartphones, the penetration of WiFi and Bluetooth enabled devices has increased significantly. There is also a major shift in the kind of applications and services that drive the data demands in networks. Online gaming, videos, real-time streaming, social networking have become very popular. In this context, it is very unlikely that the popularity of WiFi will recede after 4G technologies like WiMAX or LTE are deployed. Even from a network planning perspective, WiMAX and LTE network operators would prefer the end user devices to migrate to WiFi when they are indoor and within range of a WiFi hot-spot . This would lead to a situation where there will be a healthy mix of both WiFi and 4G devices coexisting in a given geographical area.

The chapter is organized as follows: We present the motivation in Section 7.1. We discuss the System Model used in our work in Section 7.2. In Section 7.3, we discuss the schemes to mitigate the interference due to non-collocated devices operating in adjacent channels. Section 7.4 discusses the experimental setup and the initial results for protecting transmissions in non-collocated coexistence scenario. In Section 7.5, we discuss improvements to the scheme with transmit power control. Concluding remarks and future work are discussed in Section 7.6.

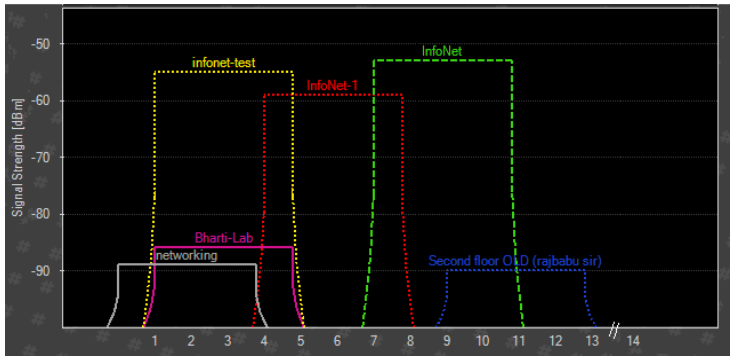


Figure 7.1: Active access points monitored using inSSIDer the Information Networks Lab, Department of Electrical Engineering, IIT Bombay.

7.1 Motivation

IEEE 802.16 WiMAX [12], is one of the 4G standards that can facilitate the last mile wireless broadband access as an alternative to cable and Digital Subscriber Line (DSL). This last mile wireless is also dominated by very dense deployment of personal and commercial WiFi access networks. WiFi uses a channel width of 22 MHz while operating in IEEE 802.11b mode and 20 MHz while operating in IEEE 802.11g/n mode [11]. The legal channels for WiFi occupy frequencies from 2400 MHz to 2484 MHz in most parts of the world. WiMAX channel bandwidths can be 1.25 MHz, 5 MHz, 10 MHz and 20 MHz depending upon the band used. WiMAX channels are in 2.3 GHz and 2.5 GHz licensed band and the exact frequencies used vary from country to country.

A typical wireless coverage map in our lab (InfoNet lab inside the Department of Electrical Engineering, IIT Bombay) is shown in Figure 7.1. The channel occupancy of wireless access points is obtained using the inSSIDer wireless analyzer tool [72]. Looking at the central frequency of the envelopes, it can be seen that there are multiple wireless networks occupying most of the orthogonal Channels 1, 6 and 11 (center frequencies 2412 MHz, 2437 MHz and 2462 MHz respectively). It is difficult to avoid channels 1 and 11 and prevent interference with 2.3 GHz and 2.5 GHz BWA networks. We also capture the spectrum utilization of these networks on a hand held spectrum analyzer (Rhode & Schwarz FSH8) to observe the out of band spillage. In Figure 7.2, we concentrate on the channel occupancy of a wireless network operating on Channel 1 of IEEE 801.11 (2402 MHz to 2422 MHz). It can be seen that the out-of-band signal received from WiFi networks is as high as -86dBm (at 2380 MHz) even at a separation of more than 20 MHz which is out side the 2.4 GHz band — Marker M3 in Figure 7.2. This is

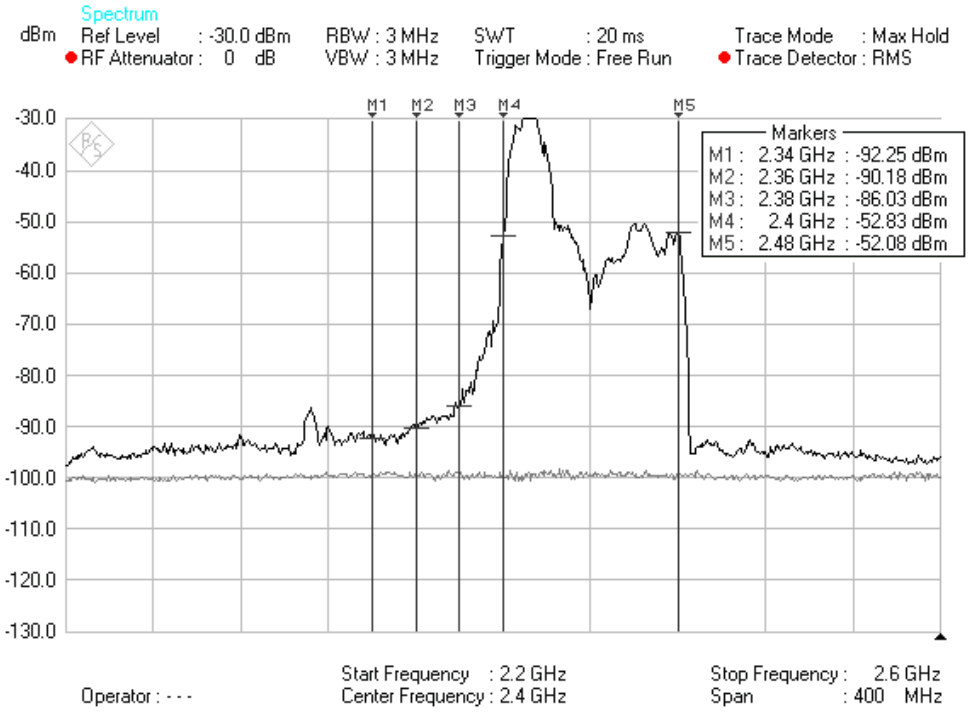


Figure 7.2: Spectrum scan in the Information Networks Lab, Department of Electrical Engineering, IIT Bombay.

a conservative estimate because the antenna used during the measurements was optimized for operations in the license-free band only (2.4 GHz).

These findings are further strengthened by the observations in [68]. It has been shown by authors in [68] that even at a separation of 114 MHz, WiFi signals can be received with signal strength of -75 dBm. This is largely due to the fact that WiFi devices use low cost filters that are not very efficient in reducing out of band spillage. Authors in [68] report that the WiFi channel at 2.412 GHz (Channel 1) generates out of band spillage of up to -61 dBm which results in an in-band interference for the adjacent 2.380 GHz WiMAX channel. Similarly 2.462 GHz (Channel 11) generates an in-band interference of levels up to -75 dBm for the adjacent 2.576 GHz WiMAX channel. This has also been independently verified by us (Figure 7.2).

WiMAX devices operate with a receiver sensitivity of -114 dBm [12]. Hence, an isolation of 53 dB is required between WiMAX and WiFi antennae in ideal conditions, where there is out of band spillage of upto -61 dBm : $|-114$ dBm - $(-61$ dBm$)|$ = 53 dB. This corresponds to a free space separation distance of around 7 m. The spectrum analyzer plots also show difference in out of band emissions generated by signal generator and actual WiFi hardware. Authors in [69] also suggest a minimum isolation distance of 7 m or an isolation of 56 dB to 60 dB when

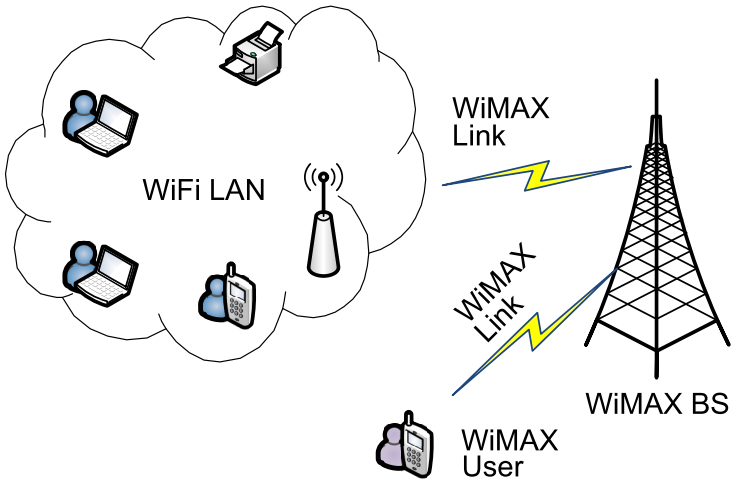


Figure 7.3: A WiMAX-WiFi Coexistence Scenario.

WiMAX and WiFi devices are in very close proximity to each other.

7.2 System Model

We consider a scenario where a network has both WiFi and WiMAX stations coexisting within close proximity. This includes situations like coffee shop hot-spots, airport hot-spots, home WiFi networks. A local WiFi network enables connectivity to a group of users in the smaller distance range of upto 100 m. The WiMAX network enables connectivity to devices like laptops and mobile phones that are clients in a range of upto 5 km. In such a scenario, some of the WiFi and WiMAX devices may be located close to each other. This could lead to adjacent channel interference causing degradation of performance in both networks as discussed in Section 7.1. A typical network setting is shown in Figure 7.3.

Collocated interference occurs when one of the radio interfaces is transmitting and another is receiving. The problem of collocated interference can be solved with the help of a simple time sharing method. As in the case of multiple wireless interfaces on a single platform, signaling between the radios can be used to coordinate the transmissions.

The interference generated by transmit and receive operations of the WiFi and WiMAX devices is summarized in Table 7.1. When both client devices on different technologies are transmitting, the corresponding receivers are assumed to be reasonably far apart. WiFi access point is typically located indoors for the hot-spot coverage and WiMAX base station is typically located outdoors on a tower and hence the corresponding receivers of the client devices are

Table 7.1: Interference matrix for WiFi and WiMAX transmissions

WiMAX \ WiFi	Transmit	Receive
Transmit	No Interference	**Interference**
Receive	**Interference**	No Interference

not affected by the adjacent channel interference. Similarly, in the case of adjacent WiFi and WiMAX devices receiving simultaneously, the corresponding transmitters are farther than the 7 m range to the other receiver and hence will not cause any problem as highlighted in Section 7.1. In cases of *WiFi device transmitting* and the *WiMAX device receiving* or *vice-versa*, the adjacent channel interference is a problem. We look at ways to mitigate this interference in the subsequent sections.

7.3 Protection for Transmissions

IEEE 802.16m Wireless Standard [73] introduces a Collocated Coexistence (CLC) class of devices. This enables measurement for interference at the WiMAX Subscriber Station (SS) and adaptation of the transmit/receive schedule at the the WiMAX Base Station (BS) depending on intereferecnce measurement reports. However, the standard just solves the problem for collocated coexistence, i.e., WiFi and WiMAX radios in the same device platform.

We assume that the Collocated Coexistence (CLC) enabled WiMAX SS is a dual radio device with both WiFi and WiMAX radio interfaces. When the WiMAX interface is in use, the spare WiFi radio interface can be used for coordination across users. This coordinator interface will allow arbitration of radio resources across multiple nodes when both WiFi and WiMAX SS devices are in close proximity to each other. The location of the multi-radio node with respect to the WiFi and WiMAX networks is shown in Figure 7.4. It is important to note that the WiFi interface of the multi-radio WiFi-WiMAX node is not associated with the WiFi access point and is just within the interference range of a potentially interfering WiFi device. The CLC Controller is a module that exists inside the multi-radio node for coordination across interfaces.

The WiFi interface in the dual-radio device will remain in promiscuous listening mode when WiMAX radio is being used. This will allow the WiFi interface to gather information about interfering nodes in the proximity and decide whether a coordination action has to be

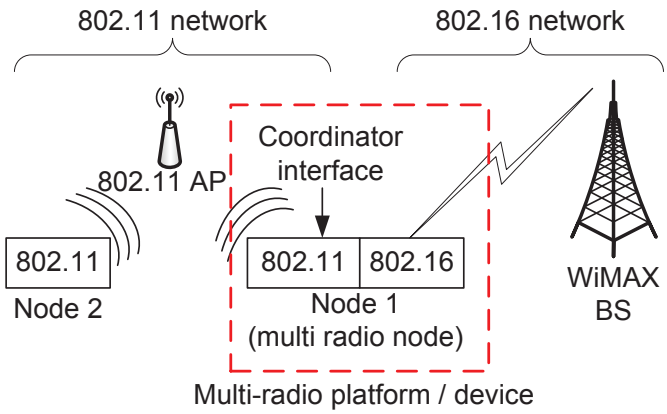


Figure 7.4: Coordinator interface and CLC

undertaken by the CLC Controller. The WiFi interface on the multi-radio platform will be referred to as the coordinator interface hence forth in this chapter. As seen in Table 7.1, when both WiFi and WiMAX are transmitting or receiving, there is no problem of adjacent channel interference. The adjacent channel interference exists only in the case of one of the devices transmitting while the other device is receiving.

The coordinator interface listens to the WiFi channel in promiscuous listening mode on channels adjacent to the one being used by WiMAX e.g., if the WiMAX SS is operating on 2380-2400 MHz channel, then Channel 1 of WiFi (2412 MHz) will be monitored and similarly if WiMAX SS is operating on 2496-2516 MHz channel, then Channel 11 of WiFi (2462 MHz) will be monitored. The coordinator interface checks for received power level of packets on the adjacent WiFi channel. If the received power is greater than the interference threshold, then the CLC Controller is informed about the action to be taken in order to protect packet receptions by both WiFi and WiMAX radios.

With the help of CLC Controller and Coordinator interface, we propose a novel scheme where one of the radios among WiFi and WiMAX has to back-off allowing the other device to continue the communication. This helps in mitigating the effects of adjacent channel interference on the transmissions and reception of packets. We deal with both WiFi and WiMAX protection separately. When the WiMAX SS is receiving a packet, we protect the WiMAX packet by inhibiting any WiFi transmission in the interference range. Similarly, when WiFi interface is receiving a packet, we protect the WiFi packet by informing the WiMAX BS to not schedule any transmissions by WiMAX SS. Both the schemes are presented in detail in the subsequent sections.

7.3.1 Protecting WiMAX Reception

The fist block in each WiMAX frame contains the schedule provided by the WiMAX BS. This control block containing the schedule is called the MAP. MAP contains both the uplink (UL-MAP) and downlink (DL-MAP) schedule to be followed. By inspecting the DL-MAP, the WiMAX SS is aware of the incoming packets in the current frame. The coordinator interface decides, based on the measurements on adjacent channels, if a WiFi device in the vicinity can potentially interfere. If a WiFi device is detected, then CLC Controller is informed about coordinating the transmissions.

In case of WiFi transmissions, the nodes determine the transmit opportunity based on a binary exponential back-off if the WiFi channel is found to be idle. The WiFi protocol provides for various control packets to ensure collision free communication. In our scheme, we exploit the behavior of WiFi nodes in hidden node situations to our advantage. WiFi uses Request-to-Send (RTS) and Clear-to-Send (CTS) packets between source and destination before a packet transmission. Both, RTS and CTS packets contain a Network Allocation Vector (NAV). The NAV indicates the total time required by the source and destination to complete the transmission. All nodes that hear the CTS packet are required to abstain from transmitting packets for a duration specified in the NAV.

Nodes that hear an RTS packet and not the CTS, can still proceed with transmissions — exposed node scenario of WiFi. However, it is mandatory for nodes to back-off all transmissions if they hear a CTS packet — hidden node scenario in WiFi. This behavior of the protocol is used to protect WiMAX SS packet reception.

Figure 7.5 shows the protection of WiMAX packet reception. The DL-MAP comprising the downlink schedule points to the WiMAX SS downlink slots in the next frame. The duration of one WiMAX frame is typically 5 ms. Just before the start of the next WiMAX frame, the CLC Controller is informed by the WiMAX interface to generate a CTS packet with NAV equivalent to the WiMAX frame duration. The CLC Controller uses the WiFi coordinator interface to transmit a CTS packet. All WiFi nodes in the vicinity of WiMAX SS that hear the CTS packet abstain from transmitting packets for the duration of the NAV, hence protecting the WiMAX SS packet reception.

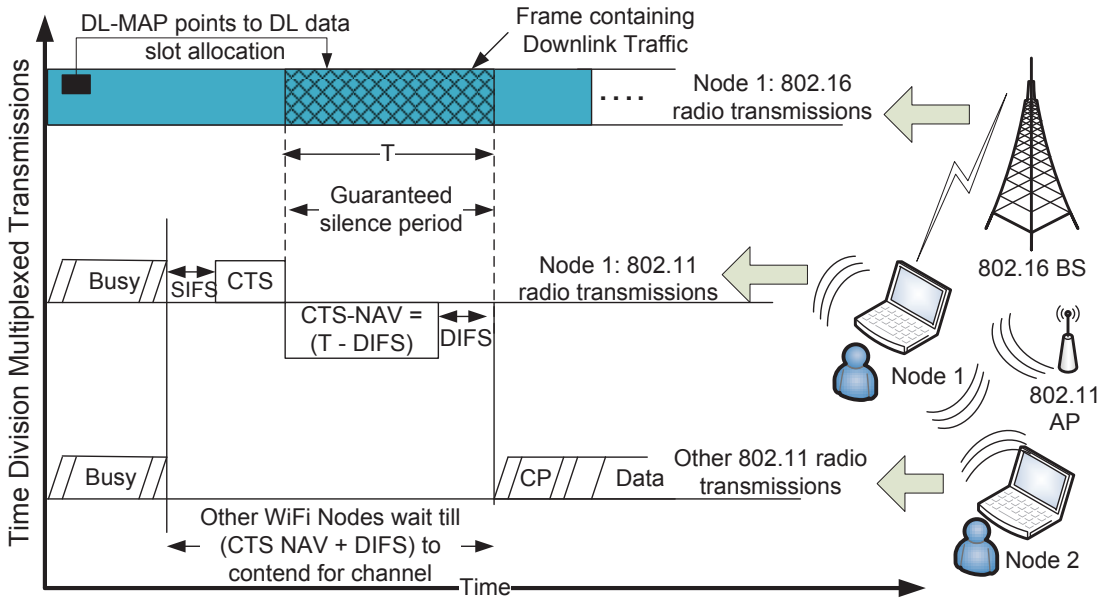


Figure 7.5: Protecting WiMAX reception

7.3.2 Protecting WiFi Reception

WiFi devices receive data and control packets that may be both periodic and aperiodic. Protecting the periodic control packets (like Beacons) is important for reliable functioning of the WiFi network (eg: multiple missed beacons leads to disconnection from the AP). Interference to the WiFi reception could be from nearby WiMAX SS. The WiMAX SS transmit slots are assigned by the WiMAX BS in the UL-MAP. WiMAX SS does have control over the time slots being used. IEEE 802.16m standard proposes a collocation aware base station scheduler. The IEEE 802.16m standard also provides special control messages for CLC, viz. CLC_Request and CLC_Report. CLC_Request allows a WiMAX SS to inform the WiMAX BS about periodic interference from collocated WiFi devices. The WiMAX BS then uses this information to schedule uplink and downlink slots for the corresponding WiMAX SS so that the WiMAX SS is not active in interfering time slots. The CLC_Report is a report generated by the WiMAX SS to give information about the collocated interference experienced by the SS. For non-periodic WiFi receptions, currently there is no provision in CLC control messages of WiMAX BS and SS. Non-periodic traffic is harder to protect because of two reasons, (a) prediction of WiFi receive instances is hard, (b) WiMAX transmit schedule is fixed in a centralized manner at the BS, and it is difficult for the WiMAX BS to predict the WiFi receive schedule for the aperiodic traffic.

We use the CLC_Report message to request WiMAX BS to allow priority to periodic WiFi

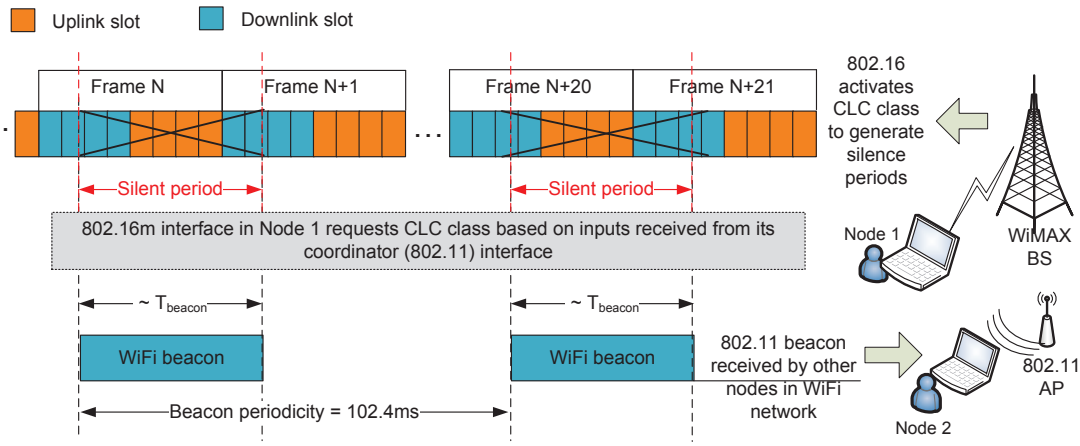


Figure 7.6: Protecting WiFi reception

receptions. The CLC_Report message requires both the duration and periodicity of the WiFi receptions that are to be protected. The duration of WiFi activity to be protected is referred to as the Silence Period. Given both the parameters, the WiMAX BS will ensure that it does not schedule any WiMAX activity for the corresponding WiMAX SS during the silence periods.

Determining the duration and periodicity of WiFi reception on a dual radio device, where both WiFi and WiMAX radios are active, is straightforward. A single control interface between the WiFi and WiMAX radios can pass on the information about channel activity across radio interfaces. However, we consider coordination across multiple devices where radio interfaces are not collocated within the same device. In both Basic mode of operation and DCF mode of operation in WiFi, the receiver WiFi node sends an ACK packet to confirm a successful packet reception. The coordinator interface listens for the ACK packets to determine the distance from the receiver. If received power of ACK packet is greater than -61 dBm as received by the coordinator interface, then the coordinator interface starts measuring periodicity of received packets. Received packets to be protected fall in two categories (a) beacon frames (periodicity of beacon frames is available as a parameter inside the beacon frames). (b) measured receive traffic with a observable periodicity, for example CBR traffic. The CLC_Request control message is then generated with the measurements generated by the coordinator interface.

Figure 7.6 shows the channel activity on WiFi and WiMAX nodes when protection is requested for periodic beacons of WiFi. Node 1 in the figure represents a dual radio node with both WiFi and WiMAX interfaces. WiFi interface of Node 1 is also the coordinator interface for CLC. Node 2 in the figure represents a WiFi node. The coordinator interface on Node 1 measures the duration and periodicity of beacon frames received by Node 2 from the WiFi

access point. This information is conveyed to the WiMAX BS in a CLC_Request packet. As seen in Figure 7.6, the WiMAX BS does not schedule any transmissions in the slots marked with 'X' for SS Node 1. This ensures that WiFi reception is protected.

The WiMAX BS can still schedule packet reception on the WiMAX SS during the silence periods because there is no impact on the packets if both WiFi and WiMAX users are receiving at the same time. The coordinator interface also ensures that the CLC_Request is generated only for packet receptions destined for Node 2. This ensures that simultaneous transmission and reception of WiFi and WiMAX is allowed.

7.4 Experimental Evaluation

The proposed scheme consists of two modules, WiMAX protection module and WiFi protection module. The WiMAX protection module sends a CLC_Report to WiMAX BS when there is an interfering WiFi device. The WiFi protection module uses the coordinator interface to send a CTS message to silence the neighboring WiFi devices. Due to unavailability of WiMAX base station for evaluation and testing, we have implemented only the WiFi protection module and emulated the WiMAX behavior. The WiFi protection module assumes a Poisson arrival of incoming packets on the WiMAX. Based on these Poisson arrivals, the coordinator interface decides to send a CTS packet with an NAV of 5 ms.

The floor plan of the testbed is shown in Figure 7.7. We are concerned with 3 nodes in the testbed labeled Nodes 1 to 3. Node 1 is the dual radio WiFi/WiMAX node, and the WiFi interface of this node is operating in promiscuous listening mode to monitor Channel 1 (2.412 GHz) of WiFi for interfering nodes. Node 2 is at a 3 m distance from Node 1. Node 3 is at a 17 m distance from Node 1 and also separated by a brick partition. Nodes 2 and 3 are connected to an access point that is placed near Node 3. This particular setup shown in Figure 7.7 is chosen specifically to replicate situations where more than one node is associated to the WiFi access point and not all WiFi nodes are interfering the WiMAX device.

7.4.1 WiFi Implementation

We need to make driver changes only in the dual radio device to enable sending of modified CTS packets. All other WiFi devices in the network do not need any changes in their drivers and operate with normal WiFi protocol stack.

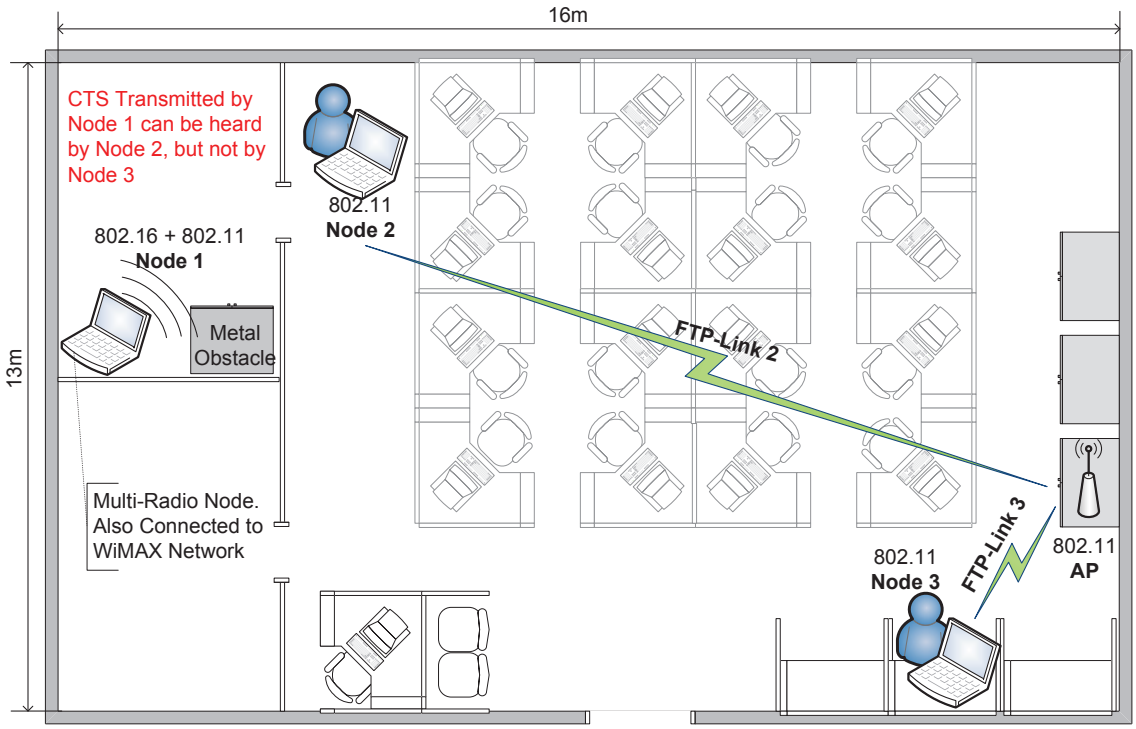


Figure 7.7: Experimental Setup inside Information Networks Lab, Department of Electrical Engineering, IIT Bombay

7.4.1.1 Challenges in Selecting Hardware for Testbed

The choice of appropriate hardware for the testbed was a challenging task. There were multiple factors to be considered for the choice for the wireless card:

Interface on PC (USB, PCI, MiniPCI): MiniPCI interface cards were ruled out as an option because of unavailability of compatible embedded boards. A Desktop based PCI card was a good candidate because of the availability of right chipset and driver. USB interface was also preferable because of portability of the USB WiFi dongles.

Full Source Code availability for Drivers: Implementation of our scheme on the coordinator interface required monitor mode support for the wireless interface and ability to patch the drivers to generate packets.

Detachable antenna: In the experimental evaluation, we had to reduce the transmit power to very low levels. Software transmit power control provided by the driver does not allow power less than 1dBm on most cards. Hence, it was essential to use external RF attenuators to reduce the transmit power.

Monitor mode support: One of the key requirements for the coordinator interface is to be able to passively monitor wireless traffic on the adjacent interfering WiFi channel and collect

statistics to assist in coexistence coordination. Only select few chipsets support Monitor mode of operation viz: Atheros [74], Realtek RT8187 [75].

Packet Injection: A key requirement of the coordinator interface is to be able to generate CTS packets with desired NAV value in order to silence interfering WiFi nodes in the adjacent channels.

Packet Injection was the most critical of the requirements driving the hardware selection. In all wireless cards, the crucial MAC control functionality like control packet generation (i.e., RTS, CTS, ACK), is implemented in the firmware. Functionality like adding correct headers and flags to DATA packets, adaptive modulation scheme selection, and channel scanning is implemented by the driver on the host device. In the event of a data packet being transmitted, depending on the RTS-Threshold, a RTS packet is generated by the firmware in the wireless card. The driver has little control over the format and contents of the RTS packet.

In the data flow of packet in the wireless card, each packet being transmitted is prepended by the PHY header and the Frame Check Sequence (FCS) field in MAC header is filled in by the firmware. This makes it difficult to generate a raw packet with CTS frame structure from the driver (which runs on the host device) and inject it into the network. Most wireless card firmwares would append a DATA packet header to the bytes being sent by the driver because the driver is not allowed to send control packets.

Atheros Chipset on Madwifi driver [62] provided with a capability to inject packets while in monitor mode. But, to overcome the limitation of wrong headers being attached to the packets by firmware, RAW packet generation library Lorcon2 [76] was used. Lorcon2 creates a virtual interface using the wireless card, making two active virtual interfaces for the card. One virtual interface in monitor mode can passively capture packets on the network, the other virtual interface in transmit mode can send custom frames. A CTS packet is created and transmitted on the air using Lorcon2.

In our experiments, it was observed that for each CTS transmission being triggered using Lorcon2, 11 copies of the packet were being transmitted on air. A wireless packet trace using Wireshark [57], confirmed that the first transmission is the original packet and all subsequent transmissions are re-transmission attempts by the hardware. This was as a result of a bug in the Madwifi driver. While transmitting any packet in monitor mode, the wireless card was waiting for a MAC layer ACK packet. In the absence of the ACK, the wireless card attempted a re-transmission of the packet. The default retransmission limit in Madwifi driver is 10, thereby

Table 7.2: Wireless Card Details

Hardware	Details
Wireless Card	TP-Link TL-WN350GD PCI card
Wireless Chipset Chipset	Atheros AR2417
IEEE Standards	54Mbps, IEEE 802.11 b/g capable
Frequency Range	2.4 GHz
Antenna Connector	RP-SMA
Maximum Output Power	18dBm
External Antenna	2 dBi

generating 11 packets for each transmission. A change in the Madwifi driver to treat monitor mode separately and allow zero retries while transmitting in monitor mode fixed the problem of multiple CTS packets.

We use a TP-Link TL-WN350GD PCI wireless card for the experiments. The detailed specifications for the hardware used for the testbed are summarized in Table 7.2.

As shown in Figure 7.7, wireless cards in Nodes 2 and 3 are setup in client mode and are configured to connect to the Access Point. Nodes 2 and 3 use are unmodified version of the wireless driver and operate in normal client mode. Node 1 is used as a coordinator interface and setup in monitor mode with Lorcon2 to inject customized CTS packets to silence the interfering nodes.

7.4.2 Initial Results for WiMAX Protection using CTS Packets by Coordinator Interface

Initially, we determine the effectiveness of the CTS packets with custom NAV duration field. As shown in Figure 7.7, we start a FTP session from Node 2 to AP and Node 3 to AP. The traffic is generated using Iperf [64] traffic generator. We configure the client nodes in IEEE 802.11g mode, set the Access Point to operate in Channel 1 (center frequency 2.412 GHz) and generate a traffic load of 5 Mbps and 15 Mbps from Node 2 and Node 3 respectively. The FTP flows remain active for a 60 s duration. The CTS packets are injected by Node 1 at 1 ms intervals with NAV of 5 ms. The CTS packet generation starts at 20 s and ends at 40 s. The FTP flows from Node 2 and Node 3 are affected by the CTS packets during the time interval 20-40 s. The

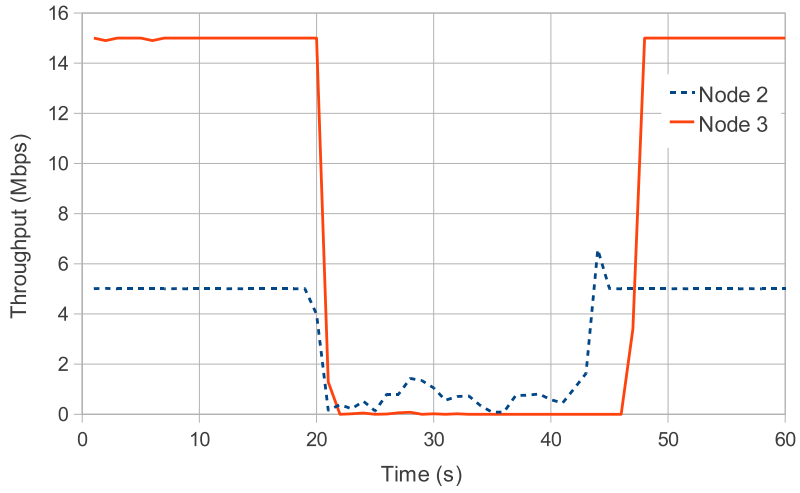


Figure 7.8: Impact of CTS Packets Transmitted by the Coordinator Interface on FTP traffic (CTS parameters: Interval=1 ms, NAV=5 ms, Power=5 dBm)

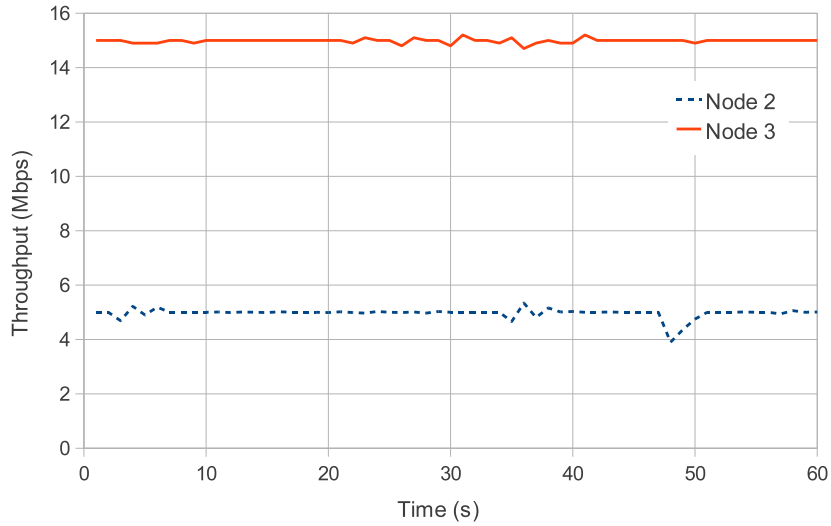


Figure 7.9: Impact of CTS Packets Transmitted by the Coordinator Interface on FTP traffic (CTS parameters: Interval=10 ms, NAV=5 ms, Power=5 dBm)

observed throughput for both FTP flows by Node 2 and Node 3 can be seen in Figure 7.8.

From Figure 7.8, it can be observed that CTS packets transmitted with a constant power can cause the entire WiFi cell in the vicinity of the coordinator interface to remain silent during CTS NAV periods. Since we are flooding the CTS packets at very high rate (1 ms intervals), and the silent period requested in the NAV is 5 ms, there is no scope for any traffic to pass through in the interval of 20s-40 s.

In the next experiment, we increase the interval to 10 ms. This allows for 5 ms silent period every 10 ms. The results are shown in Figure 7.9. It can be seen that there is very less

impact on the throughput of the FTP sessions even with very high rate of CTS packets. With CTS packets every 10 ms and requesting a silent period of 5 ms each, approximately 50% of the air time is reserved in silent periods. As seen in [77] and the references therein, the effective usable throughput from an IEEE 802.11 wireless network is less than 60% of the PHY data rate due to protocol overheads. These protocol related overheads result in idle time being spent by nodes either in Back-off or in protocol mandated silent periods like DIFS and SIFS. Since the total load on the system is 20 Mbps (15 Mbps + 5 Mbps), there is enough spare time to accommodate the requested silent periods without affecting the throughput of data flows.

Discussion

It can be seen from Figures 7.8 and 7.9, that no power control on the CTS transmissions by coordinator interface leads to situations where entire adjacent cell is silenced during CTS NAV periods. This is undesirable as the intent is only to block the interfering node in the vicinity of coordinator interface to remain silent.

It is observed that:

1. CTS packets, transmitted by the coordinator interface, are effective in creating silent zones without any modification in the STA drivers,

2. CTS packets intervals can be very small and still not affect the throughput of the adjacent wireless network.

The former observation is just an assertion that the CTS scheme works. The latter observation is more important, because the CTS transmissions by the coordinator interface can be used in moderation to protect WiMAX frames without affecting the WiFi network throughput significantly.

7.5 Transmit Power Control by Coordinator Interface in the Protection for WiMAX Reception

The results in Section 7.4.2, show that if the CTS packets from coordinator interface are triggered very frequently, then it could lead to the entire adjacent WiFi network to suffer. We extend the scheme proposed in Section 7.3.1 to enable adaptive transmit power control of the

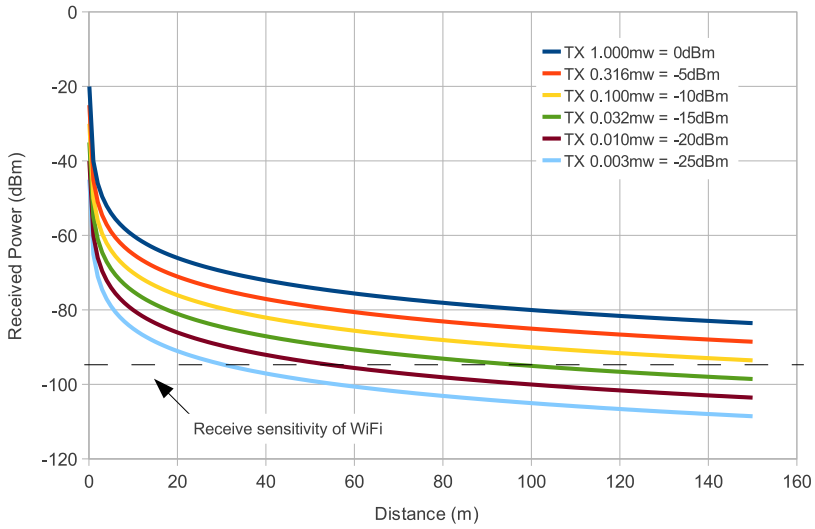


Figure 7.10: Free Space Pathloss with Varying transmit power

CTS packets. This allows us to limit the extent of silence zone requested by the CTS packets and hence improving the system throughput of the adjacent WiFi network. The pathloss in dB can be computed as,

$$\text{pathloss} = 10log_{10}\Big[\Big(\frac{4\pi d}{\lambda}\Big)^2\Big], \tag{7.1}$$

Where λ is the wavelength of the signal being transmitted. In our case, for a 2.4 GHz WiFi signal, the wavelength is

$$\lambda = \frac{3.8 \cdot 10^8}{2400 \cdot 10^6} = 0.125\ m.$$

From (7.1), the received power can be computed as, $P_{received} = P_{transmit} -$ pathloss. Figure 7.10 shows the pathloss for different transmit powers in multiples of 5 dBm steps from a transmit power of 1 mW or 0 dBm. The figure also indicates the noise floor for WiFi devices. The receive sensitivity of WiFi is approximately -96 dBm, i.e. any signal with receive signal strength indicator (RSSI) greater than -96 dBm can be decoded by the WiFi device. Hence, WiFi devices that are located as far as 100 m from the coordinator interface will be able to receive the CTS packets. As a result, all the nodes that receive the CTS packet are forced to remain silent for the WiMAX packet reception at the dual radio node, which is undesirable. Given that the typical range of a commercial WiFi AP is 100 m, we need to transmit the CTS packets at lower transmit powers to limit the silence zone.

As discussed in Section 7.1, the interference from adjacent channel is significant only for a physical separation of 7 m between interfering devices. CTS packets that are received beyond 7 m will not help the WiMAX reception in any way. So, these CTS packets will only decrease

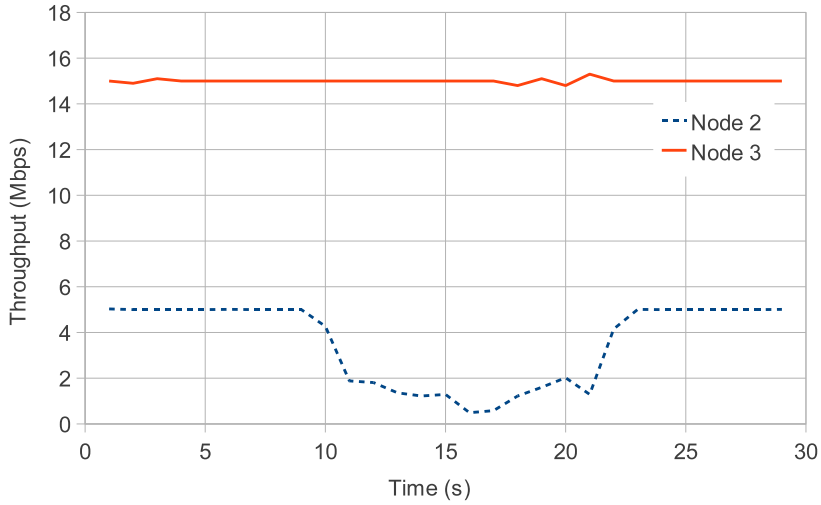


Figure 7.11: Impact of CTS Packets Transmitted by the coordinator Interface on FTP traffic (CTS parameters: Interval=1ms, NAV=5 ms, Power=-20 dBm)

Table 7.3: Throughput achieved with CTS transmit power = $-20\ dBm$

CTS Interval	**1 ms**	**10 ms**	**20 ms**	**100 ms**
Node 2	1.34 Mbps	5.002 Mbps	5 Mbps	5 Mbps
Node 3	15 Mbps	15 Mbps	15 Mbps	15 Mbps

the system throughput of the adjacent WiFi network. Theoretically, it can be seen that we need to transmit CTS packets at powers below -20 dBm to control the impact of silence zone created.

7.5.1 Impact of Variable CTS Power Control

The current wireless drivers do not allow packet transmissions at powers below 1 mW (0 dBm). Hence, for the purpose of this study, we attach RF attenuators to the coordinator interface to reduce the transmit power below 1 mW.

Figure 7.11 shows the results for transmission of CTS with power -20 dBm and interval of 1 ms. Comparing the results with Figure 7.8, where no power control is used, the FTP flow for Node 3 is unaffected by the CTS packets. Node 3 is located at a distance of approximately 17 m separated by a few wooden partitions. This allows enough margin for Node 3 to ignore the CTS packets and continue its transmissions. It should be noted that the CTS packets are injected in the network at a very high rate (interval of 1 ms and NAV of 5 ms), and in actual practice the interval will be higher. This will result in better throughput for Node 2 in normal circumstances. This also ensures that only the nodes that are in the vicinity of the coordinator

interface and hear the CTS packets remain silent for the duration of CTS transmissions. Table 7.3, shows a summary of throughput achieved for various CTS intervals. It can be seen that the throughput of Node 2 is affected only when CTS intervals are very low. The results in Table 7.3 are for the duration between 10 s and 20 s as seen in Figure 7.11 when CTS packets are being transmitted.

We illustrate the performance impact on WiFi throughput due to the CTS packets with an example. Consider a WiMAX SS with a downlink load of less than 2 Mbps, and a WiMAX system throughput of at least 12 Mbps (minimum SINR = 12 dB, minimum modulation scheme 16QAM-3/4). In the best case scenario, downlink subframes optimally packed by the BS in as few frames as possible, the WiMAX SS needs one out of every six frames to be protected. In this case, the CLC controller will generate a CTS packet every 30 ms (one frame = 5 ms). In an average case, when the downlink subframes for the WiMAX SS are not optimally packed, the CLC Controller may need alternate WiMAX frame to be protected. The CTS interval in this case would be 10 ms. From the results in Table 7.3, it is clear that the WiFi network performance would not be affected in both the cases.

7.6 Summary

We have demonstrated how an additional IEEE 802.11 radio interface, on a multi-radio platform (IEEE 802.11 and IEEE 802.16 interfaces), can be used effectively to mitigate adjacent channel interference. We also demonstrate that the CTS-to-Self packets generated by the coordinator interface to protect WiMAX transmissions do not affect the performance of the WiFi network operating in the adjacent channels. We also demonstrate, with experimentation, that power control can be used effectively to limit the silence zone created by CTS-to-Self packets triggered by the WiMAX transmissions. We have proposed a scheme to protect WiFi transmissions by invoking CLC messages to the IEEE 802.16 BS to modify its schedule according to the WiFi activity.

Chapter 8

Summary and Future Work

In this chapter we summarize and discuss the main contributions of the thesis. We also discuss possible extensions to this work and open problems.

8.1 Main Contributions of the Thesis

The main contribusions of the thesis are as follows:

1. **Analysis of IEEE 802.11 based network in Non-Saturation condition with homogeneous arrivals across client nodes**. We use the fixed point method to determine collision probability, attempt rate and queue status. Using these, we determine closed form expressions for the time between two successive packet departures from an IEEE 802.11 cell (the exit process). In the homogeneous case, each client device associated with the access point is assumed to have identical arrival process. We validate the results from the analytical model using QualNet simulations.

2. **Extension of the Non-Saturation IEEE 802.11 analysis for non-homogeneous case where client nodes connected to the access point have different arrival rates**. A multi-variate fixed point method is used to determine collision, attempt and queue status probabilities for nodes in the network. We also determine the mean departure time and the variance in the departure times for this condition. We validate the analytical model using QualNet simulations.

3. **Setting up an Experimental testbed for validating the Non-Saturation IEEE 802.11 homogeneous and non-homogeneous analytical models**. We collect statistics from the

wireless drivers for various metrics like collisions, inter packet times and waiting times to verify the analytical model. In order to achieve accurate results, modifications are made to the wireless drivers to enable the logging of statistics across different nodes in a time synchronized manner. The results obtained from the analytical model are found to follow the trends observed in testbed results.

4. **Analysis of a hybrid IEEE 802.16, IEEE 802.11 network based on Time Division Multiple Access (TDMA) scheduling on the uplink**. The backhaul network with TDMA scheduling is modeled as a GI/D/1 queue. The arrivals to the GI/D/1 queue are generated using the exit process derived in IEEE 802.11 exit process. We determine performance indicators for queue length and waiting times at the backhaul network for safe operation regions. We validate the analytical model using QualNet simulations.

5. **Studying the issues of coexistence of non-collocated IEEE 802.11 and IEEE 802.16 networks while operating in adjacent channels**. We have proposed solutions to mitigate the coexistence issues enabling both IEEE 802.11 and IEEE 802.16 networks to operate simultaneously in close proximity. A simple solution based on Clear to Send (CTS) message with power-control is proposed in a dual-radio (IEEE 802.11 and IEEE 802.16) node to disable transmissions from an interfering IEEE 802.11 device. We have implemented the proposed scheme on IEEE 802.11 testbed to verify the effectiveness of the scheme.

8.2 Open Problems and Future Work

8.2.1 IEEE 802.11 Performance Modeling

In the case of IEEE 802.11 network analysis, we model the MAC layer protocol in both the saturated and non-saturated conditions. We have also modeled the performance for identical arrivals at each node and non-identical arrivals. There are a few more factors that may impact the performance of an IEEE 802.11 single cell network performance, viz:

- impact of the PHY layer condition,
- impact of realistic traffic like Hypertext Transfer Protocol (HTTP) and web traffic on the network performance,

- impact of interference due to other WiFi networks on the performance.

8.2.1.1 Impact of the PHY layer

PHY layer channel varies rapidly over time. This causes two situations of concern (a) the available data rate to individual nodes changes over time, and (b) packets transmitted may get corrupted due to temporal disturbances.

The time varying nature of the channel, and hence the varying choice of modulation schemes adds one extra dimension to the capability of a node's ability to attempt transmission of a packet in addition to idle channel availability. Depending on the available Signal to Interference Noise Ratio (SINR), the choice of modulation scheme may change for the wireless devices. However, in practice, the IEEE 802.11 protocol behaves differently. The modulation scheme choice is dependent on failed packet transmission attempts at higher modulation schemes. As we attempt to be more realistic in the modeling of the wireless network performance, the analytical model gets more complex.

The temporal corruption of wireless packets is a more simpler problem to address. This can be modeled in a similar fashion as a collision due to multiple nodes transmitting at the same time.

8.2.1.2 Impact of realistic web traffic

Real world traffic model for the packet arrivals in the non-saturated case analysis of networks makes a model more realistic and accurate. However, the web browsing patterns do not lend themselves well to any single elegant mathematical model. There are various approximations of the web traffic based on measurement data at edge routers of networks. A Pareto distribution [78] or a Zipf [79] distribution may model the web traffic closely. However, these have their own limitations. Both Pareto and Zipf distributions approximate the file sizes that an average web browsing session might come across, but in the case of a MAC layer modeling, we need to look at individual packets. So, any file size larger than the Maximum Transfer Unit (MTU) of the wireless network needs to be fragmented into individual packets before considering for analysis. This makes it difficult for the web traffic models to be directly incorporated into the performance model of a network.

8.2.1.3 Impact of interference

Interference from other IEEE 802.11 networks may cause degradation in performance of the IEEE 802.11 network under consideration. Consider a simple scenario of data packet transmissions from the interfering network causing the wireless channel to be busy. A trivial method to address this could be to consider both the network under consideration and the interfering network as a single large network and then model the behavior. However, the analysis becomes more complex when the interference is on adjacent non-orthogonal channels. Also, the geographical area under consideration for the network can become significantly large because one may have to consider interference to every edge node in the network.

8.2.2 Coexistence of IEEE 802.11 and 4G Technologies

The coexistence of IEEE 802.11 and 4G Technologies like WiMAX and LTE will only increase with time as more 4G devices enter the market. We study the performance impact in light and moderate load networks and in the cases where the IEEE 802.11 (WiFi) network is indoors. Heavy load and outdoor WiFi networks need to be addressed to solve the coexistence problem convincingly.

In cases of heavy load networks, the coordinator interface may not get opportunities to seize control of the channel. This may lead to a situation that even with a coordination algorithm in place the network operates without any protection to frames and losses are observed due to interference.

Outdoor WiFi networks present a different set of challenges. Indoor WiFi networks have lower transmit powers at both the WiFi access point and the WiFi client. This allows easier control over the silence zone created for the purpose of coordination. However, in cases of outdoor networks like campus wide WiFi or City-wide WiFi networks the area covered by a single access point is much larger as compared to indoor access points. If the coordinator interface ends up being close to an outdoor access point, a very large area gets silenced resulting in significantly degraded WiFi performance.

The scheme proposed addresses the basic method for achieving protection of WiFi and WiMAX frames in the wireless domain. The issue of fairness and degree to which protection may be used for WiFi and for WiMAX can be evaluated from the perspective of fair access to the channel resources given that adjacent channel devices are timesharing the channel in the

case of heavy-interference situations.

Methodologies available for protection mechanisms in WiMAX, LTE and LTE-Advanced may differ based on the protocol features available. In this thesis, we propose and evaluate the effectiveness of a scheme for WiFi-WiMAX coexistence. Although we believe that the schemes can largely be applicable for both LTE, LTE-Advanced and other technologies, the efectiveness of the schemes and implementation specific details need to be worked upon.

Appendix A

Brief Primer on IEEE 802.11 MAC

We introduce the IEEE 802.11 protocol in this chapter. This chapter provides a brief overview of the essential protocol details that will help in understanding the analytical model and experimental results in the thesis. This chapter is not intended to be a detailed literature regarding the IEEE 802.11 protocol. Interested readers can refer to [80] [11] and references therein for a detailed introduction to the IEEE 802.11 protocol and the wireless local area network communication standard.

This chapter is divided into the following sections for a general overview of the IEEE 802.11 protocol:

- The Backoff process
- Various packet formats and structures
- Timing, Counters and Variables
- Two modes of packet exchange in IEEE 802.11

A.1 Backoff process

The IEEE 802.11 protocol works on a Slotted Aloha [81] principle for multiple access along with Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Consider there are N nodes in the wireless network, each node within transmission range of each other and wanting to transmit a packet. Every node will attempt to transmit only at discrete slot boundaries. These slot boundaries are not synchronized across each node and all communication happens in an

asynchronous manner. The slot is the minimum amount of measurable time in an IEEE 802.11 wireless system.

Every node that has a packet to transmit, checks if the wireless medium is not busy with some other transmission. If the medium is found to be idle, then the node waits for a random number of slots checking every time if the wireless medium is still idle. If the medium is still found to be idle, the node transmits the packet which is followed by an acknowledgement packet from the receiver. The activity of waiting for random amount of slots before attempting to transmit a packet is called as the *backoff* process in IEEE 802.11.

IEEE 802.11 specifically follows the binary exponential backoff. Figure A.1 shows a simple backoff process in an IEEE 802.11 network. As seen in the figure, it can be seen that three nodes having a packet to transmit choose different number of backoff slots. Node 2 that has the least amount of backoff count of slots finds the channel to be idle at the end of backoff countdown and begins transmission of the packets.

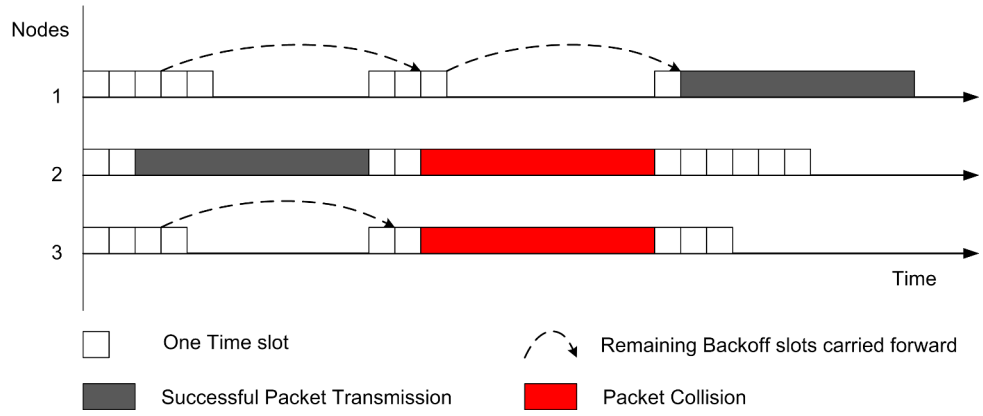


Figure A.1: Simple Backoff process in IEEE 802.11 Network

At this point, the other nodes in the network detect that the wireless medium is no longer idle and freeze the backoff countdown till such time the medium is once again free. This is the *Carrier Sense* part of the protocol. Now, at the end of packet transmission by Node 2, Nodes 1 and 3 resume the countdown from the frozen value, and Node 2 chooses a new count for the next packet. If more than one node have the same backoff count value, then all the nodes that have exhausted the countdown transmit at the same time resulting in a packet collision.

The packet collision happens on the wireless medium, and unlike the wired network, there is no mechanism for the transmitting source node to detect if a collision has happened. The only mechanism available with the source node to detect a packet collision is an acknowledgement packet from the receiver of the packet. Absence of the acknowledgement is assumed to be

collision and the packet is retransmitted by the node. In order to retransmit a collided packet the node may choose a different backoff countdown value. This new backoff countdown value is chosen according to the binary exponential backoff process.

A.1.0.1 Binary Exponential Backoff (BEB)

The binary exponential backoff mechanism is used to determine the amount of backoff count to be chosen by nodes in the network. A backoff count is chosen using the uniform distribution [82] from a range of values. The range is increased in an exponential manner every time a collision is encountered by the node. In order to determine the backoff count two variables are defined:

Contention Window - Minimum (CW_{MIN})

This is the minimum range from which the backoff count will be chosen.

Contention Window - Maximum (CW_{MAX})

This is the maximum range for choosing the backoff count and increasing the backoff count by twice after each collision.

Algorithm 1 Binary Exponential Backoff in IEEE 802.11

{initialization}
$CW_{MIN} = 31, CW_{MAX} = 1023, K = 1, CW = CW_{MIN}$
while $TRUE$ **do**
  {determine current contention window}
  $CW = 2^K * (CW_{MIN} - 1) + 1$
  $CW = max(CW, CW_{MAX})$
  if packet transmission is successful **then**
    {reduce the contention window to minimum value on success;}
    $K = 1;$
  else
    {double the contention window on every collision;}
    $K = K + 1;$
  end if
end while

In the binary exponential backoff procedure, shown in Algorithm 1, each node in the network initializes the backoff contention window to CW_{MIN}. Before attempting to transmit a packet, a random value is chosen from the range [0 - CW]. If the packet transmit attempt results in a collision, then the contention window is doubled and the backoff is chosen from the new range. This doubling of the contention window keeps happening till the contention window reaches the maximum value CW_{MAX}. Then the contention window remains at the maximum value for the maximum number of retries allowed for the packet or till such time the packet is successfully transmitted. On a successful transmission of the packet, the contention window is reinitialized to CW_{MIN}.

In order to establish whether a packet is successful or has resulted in a collision, the IEEE 802.11 protocol makes use of a Medium Access Control (MAC) layer acknowledgement for each packet. Details of the specific packet sequences and formats are in Section A.2 and A.4.

A.2 Packets

The IEEE 802.11 protocol specifies various packets for different protocol functions. There are broadly two types of packets, (a) Control packets (b) Data packets. The control packets help in coordination and control of the protocol features and help in distributed access control and collision avoidance for the medium access. The data packets are used to transport the payload from the source to the destination.

A generic IEEE 802.11 packet format is as shown in Figure A.2.

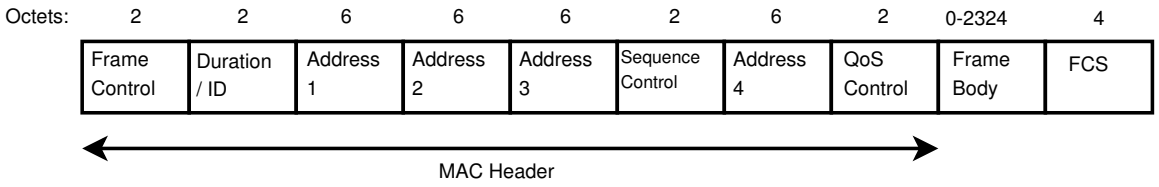


Figure A.2: Generic IEEE 802.11 frame

In the interest of brevity, we do not introduce every field in the generic frame type in this chapter. For the sake of understanding the analysis and experimental evaluation, we introduce only relevant details in the packet formats and refer the reader to IEEE 802.11 standards [11] for further details. The various control and data packets are described in this section.

A.2.1 Control Packets

The control packets are responsible for (a) distributed coordination among various nodes in the network and (b) reliable transmission of packets at the MAC layer in the network. All the control packets in the network are transmitted at the base data rate, i.e., 1 Mbps in the case of IEEE 802.11b and 2 Mbps in the case of IEEE 802.11g.

A.2.1.1 Request To Send (RTS)

The Request to Send (RTS) packet is sent by the source node in the network to indicate that the node has packet to send to a specific destination. This packet contains details about the length of the data payload to be transmitted, the intended destination, capabilities of the source node among other details. The format of the RTS packet is shown in Figure A.3.

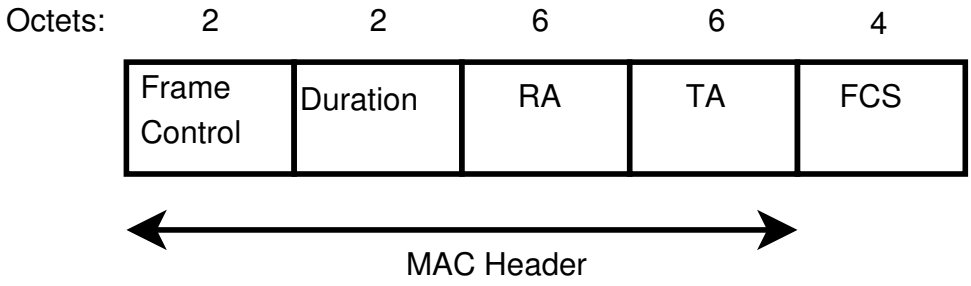


Figure A.3: IEEE 802.11 RTS packet

The length of the RTS packet is 20 Bytes. The RA field denotes the receiver address (48 bit MAC address of the receiver node) and the TA field denotes the transmitter address (48 bit MAC address of the transmitter node). The duration field denotes the combined duration required in time slots for the entire packet transmission from the source to destination.

Any node in the network that listens to the RTS packet and is not the intended recipient of the packet will wait for a pre-determined amount of time (RTS Timeout), introduced in Section A.3. If the node detects a DATA packet transmission, then the node refrains from initiating its own packet transmission in the network.

A.2.1.2 Clear To Send (CTS)

The Clear to Send (CTS) packet is sent by the receiver node in the network in response to the RTS packet. The CTS packet denotes to the source that the receiver node is not blocked

by interference from any other parallel transmission in the network and can receive the packet without any problems. The format of the CTS packet is shown in Figure A.4.

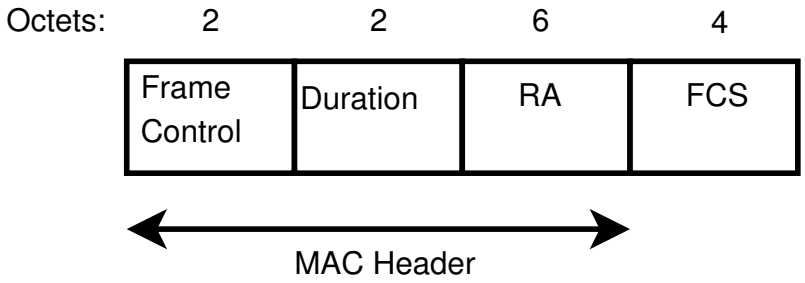


Figure A.4: IEEE 802.11 CTS packet

The length of the CTS packet is 16 Bytes. The RA field in the CTS packet is copied from the TA field of the RTS packet, i.e., the address of the receiver node in the packet transmission.

As per the IEEE 802.11 protocol, any node that receives the CTS packet and is not the intended recipient of the packet remains silent and refrains from sending any packet for the duration specified in the duration field. This combined with the carrier sensing at the source nodes ensures that the packet transmission in the network happens with fewer collisions, i.e., the only collisions that remain are as a result of choosing equal backoff count value.

A.2.1.3 ACK Packet

This packet is transmitted by the receiver node in the network after successfully receiving and decoding the DATA packet. This packet denotes the end of a successful packet transmission transaction. The format of the ACK packet is shown in Figure A.5.

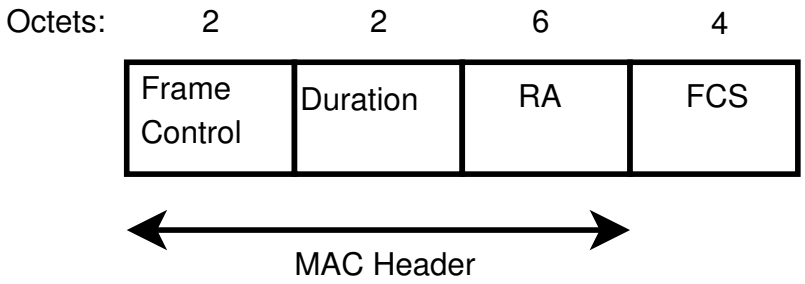


Figure A.5: IEEE 802.11 ACK packet

The length of the ACK packet is 16 Bytes. The RA field in the ACK packet is the address of the receiver node in the network. As highlighted in Section A.1, the contention window is reduced to CW_{MIN} on receiving the ACK packet.

A.2.2 Data Packets

The data packet carries the payload or data bits between the source and destination in the network. The format of the DATA packet is shown in Figure A.6.

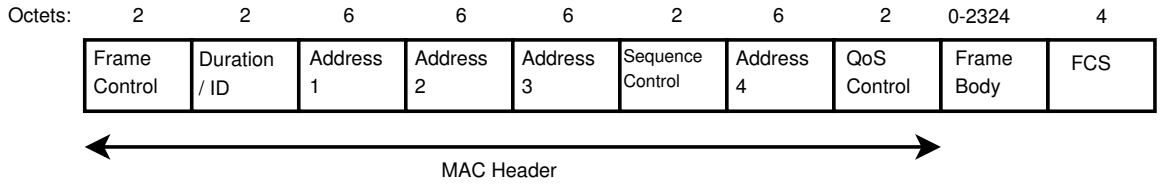


Figure A.6: IEEE 802.11 DATA packet

The length of the DATA packet can range from 36 Bytes to 2360 Bytes depending on the amount of payload being carried by the packet. The DATA packets are transmitted using the maximum data rate possible between the source and the destination nodes as per the IEEE 802.11 protocol and the history of packet exchanges between the two nodes. If the packet transmission history denotes poor signal strength, then a conservative modulation scheme may be used. The choice of modulation scheme and the adaptive fall-back to conservative modulation is vendor dependent and may vary across different implementations of the IEEE 802.11 protocol.

The IEEE 802.11 protocol defines a configurable parameter $RTS_{Threshold}$. Any packet that is larger than the $\text{RTS}_{\text{Threshold}}$ will result in the RTS packet being generated for packet transmission. The specific packet exchange with and without the RTS packet is given in Section A.4.

A.3 Timings, Counters and Variables

The IEEE 802.11 protocol defines several parameters to define time between different events and configurable parameters for performance of the protocol. The parameters defined in this section depend on the IEEE 802.11 variant (e.g., IEEE 802.11b or IEEE 802.11g). Also, certain variables depend on the specific configuration of the hardware or the drivers irrespective of the IEEE 802.11 variant being used.

A.3.1 Timings

The minimum amount of measurable time in IEEE 802.11 protocol is the slot time. The slot time differs depending on the IEEE 802.11 variant (IEEE 801.11b, IEEE 802.11g). The duration

of the slot time directly influences the protocol efficiency and the maximum achievable system throughput of the network because the amount of idle time spend by the network in backoff is dependent on this.

The slot time depends on (a) ability of the physical layer of the IEEE 802.11 hardware to make a clear channel assessment (CCA), (b) switching time from transmit mode to receive mode and vice-versa in the hardware and (c) propagation delay between transmit and receive operations between the source and the receiver. In the case of IEEE 802.11b the slot time is $20\,\mu s$ and for IEEE 802.11g the slot time is $9\,\mu s$.

A.3.1.1 Short Interframe Space (SIFS) Time

The Short Interframe Space (SIFS) denotes the smallest amount of interval between a DATA packet and the acknowledgement (ACK). This is a fixed value dependent on the IEEE 802.11 variant being used. In the case of both IEEE 802.11b and IEEE 802.11g, the SIFS time is defined as $10\,\mu s$.

A.3.1.2 DCF Interframe Space (DIFS) Time

The DCF Interframe Space (DIFS) denotes the minimum amount of time a node has to wait before getting access to the wireless medium. Any node that wishes to transmit a packet waits for a idle channel for at-least DIFS period before starting the backoff countdown and packet transmit process.

The DIFS period is defined in terms of the Slot time and the SIFS time as

$$\text{DIFS} = \text{SIFS} + 2 * \text{Slot Time}.$$

Based on the values for Slot time and SIFS, DIFS is $50\,\mu s$ and $28\,\mu s$ for IEEE 802.11b and IEEE 802.11g respectively.

A.3.1.3 Discussion

The interrelation between the various times is shown in Figure A.7.

A.3.2 Counters and Variables

The IEEE 802.11 standard defines several counters and variables to fine tune the protocol performance. The following list gives a brief summary of the various variables and counters.

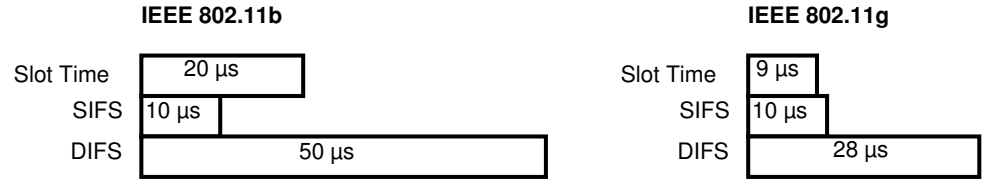


Figure A.7: IEEE 802.11 Timings

RTS Threshold

The RTS Threshold determines the minimum number of bytes of DATA that is required to initiate a DFC mode of packet transmission. If the DATA is larger than RTS Threshold, then RTS packet is transmitted by the source for the packet exchange. If the DATA is smaller than the RTS Threshold, then the packet exchange takes place in Basic mode of operation. The DCF and Basic mode of operation are defined in Section A.4.

Short Retry Limit

This counter denotes the number of times a packet that is smaller than the RTS Threshold or a Control packet is retransmitted (e.g., RTS packet). After the number of retransmission attempts cross this limit the packet is discarded. Typically the default value for Short Retry Limit is 7.

Long Retry Limit

This counter denotes the number of times a packet that is larger than the RTS Threshold will be retransmitted before being discarded. Typically the default value for the Long Retry Limit is 4.

A.4 Packet Exchange

The IEEE 802.11 protocol specifies two methods of packet exchange, (a) the Basic mode and (b) Distributed Coordination Function (DCF) mode. Both these modes provide different trade-offs during transmission in terms of successful transmission and control packet overhead.

A.4.1 Basic Mode

The Basic mode of operation in IEEE 802.11 is shown in Figure A.8. The Basic mode of operation involves directly transmitting the DATA packet from the source to the destination. This type

of frame exchange is typically used when there is very less interference in the neighborhood or when the packet sizes are small.

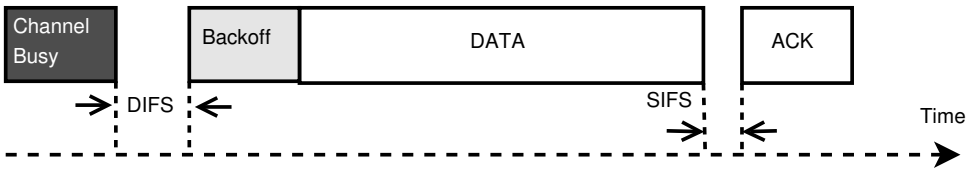


Figure A.8: IEEE 802.11 Basic Mode of operation

As seen in the figure, a node that intends to transmit a packet waits for the channel to be idle, indicated by the end of Channel Busy period. Once the channel is idle, the node waits for a duration equal to DIFS. If the medium is still idle, then the backoff countdown at the source node starts. The backoff counter is reduced by one in every slot time that is elapsed. If the medium is still idle at the end of the backoff countdown, then the node proceeds to transmit the DATA packet to the destination. After the transmission of the DATA packet, the source node waits for an ACK packet from the destination of the packet. If the packet is successfully transmitted to the destination without any collision, then the receiver responds with an after waiting at-least for SIFS amount of time. If the source does not receive an ACK after ACK Timeout duration, then the packet is assumed to have collided and retransmission of the packet is initiated with doubling of the contention windows as per the Binary Exponential Backoff (Section A.4).

A.4.2 Distributed Coordination Function (DCF) Mode

The Distributed Coordination Function (DCF) mode of operation in IEEE 802.11 is shown in Figure A.9. The DCF mode involves a two-way handshake between the source and the destination nodes before the actual DATA packet transmission takes place. This is done in order to perform Collision Avoidance on the wireless channel. Any node in the network that can listen to either the RTS or the CTS control packet waits for the entire transaction of RTS-CTS-DATA-ACK to complete before trying to access the channel.

As seen in the Figure, the actual DATA packet is transmitted only after receiving a CTS packet from the intended receiver of the packet. Just like the basic mode of operation, the source node waits for DIFS and the backoff countdown before transmitting the RTS packet. If there is no CTS reply from the destination for RTS Timeout, then the RTS is assumed to have collided

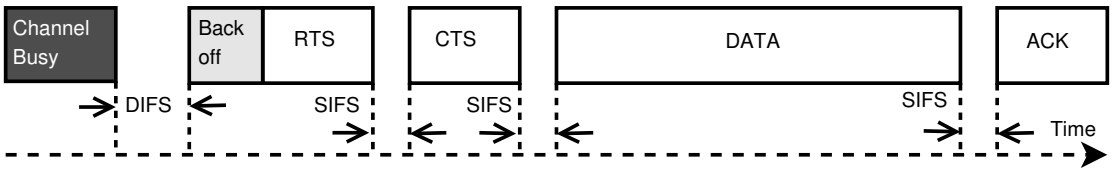


Figure A.9: IEEE 802.11 DCF Mode of operation

and a retransmission of the RTS packet takes place.

If there is a CTS packet in reply to the RTS packet from the destination, then the source node transmits the DATA packet. If the CTS packet is received correctly by the source, it can be assumed that all nodes in the vicinity of the source and destination have heard the handshake of control packets and will not attempt to transmit any packet. After the DATA packet is transmitted by the source, the receiver replies with an ACK packet to complete the transaction.

A.4.2.1 Discussion

The Basic mode of operation saves on control packet overhead during the packet exchange at the cost of loosing the entire DATA packet in the event of a collision. In contrast, the DCF mode of operation ensures that the maximum time wasted in the event of collision is equal to the size of the RTS control packet. This extra safety in the transmission comes at the cost of extra control packet overhead with RTS and CTS packets. It is also important to note that both RTS and CTS packets are control packets that are transmitted at the base data rate that consumes more time on the air while transmitting the packets. Hence, the overall system overhead increases as a result of using the DCF mechanism. The effective performance gain of using the DCF mode as compared to Basic mode of operation is situation dependent, and varies from topology, traffic pattern of users and interference from neighboring IEEE 802.11 networks.

A.5 Summary

This Chapter is meant to provide a brief overview of the IEEE 802.11 protocol with specific focus on introducing aspects that will be useful in understanding the analytical model and experimental evaluation of the IEEE 802.11 protocol in this thesis. A more detailed introduction to the IEEE 802.11 protocol and features can be found in the IEEE 802.11 standards [11].

Bibliography

[1] "Unique Identification Authority of India." [Online]. Available: http://uidai.gov.in/ 1

[2] "Census of India 2011 - Rural Urban Distribution of Population." [Online]. Available: http://censusindia.gov.in/2011-prov-results/paper2/data_files/india/Rural_Urban_2011.pdf 1

[3] "The Indian Telecom Services Performance Indicators (January March, 2013)." [Online]. Available: http://www.trai.gov.in/Content/PerformanceIndicatorsReports.aspx?ID=1&qid=1 1

[4] "Bridging the Digital Divide, Electronic Networking for Rural Asia/Pacific (ENRAP), by The International Fund for Agricultural Development (IFAD)." [Online]. Available: http://www.ifad.org/evaluation/public_html/eksyst/doc/profile/pi/enrap.pdf 2

[5] "Rural Telephony for Rural Development, Kurukshetra, A Journal on Rural Development, January 2012, Ministry of Rural Development." [Online]. Available: http://yojana.gov.in/cms/pdf/Kurukshetra/English/2012/January.pdf 2

[6] "Reaching Out to Rural India, (Feature Stories, TATA Group, India)." [Online]. Available: http://www.tata.com/company/articles/inside.aspx?artid=m73PWlDIJmU=#tata_tele 2

[7] "Thinking Blue Sky - article in Business Today, 8 August 2010." [Online]. Available: http://businesstoday.intoday.in/storyprint/5855 2

[8] "Habitation in Rural and Urban Areas, All India School Education Survey, MHRD, India." [Online]. Available: http://aises.nic.in/documents/pdf/reports/3RD_AISES/305.pdf 3

[9] S. S. Rao, "Bridging Digital Divide: Efforts in India," *Telematics and Informatics - Special issue: The World summit on the information society (WSIS) from an Asian-Pacific region perspective*, vol. 22, no. 4, pp. 361–375, November 2005. 3

[10] K. Keniston and D. Kumar, *Bridging the Digital Divide : Lessons from India*. SAGE, London, 2004. 3

[11] "IEEE Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks — Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2012*, 2012. 4, 14, 15, 23, 73, 89, 113, 116, 123

[12] "IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Broadband Wireless Access Systems," *IEEE Std 802.16-2009*, 2009. 4, 15, 78, 89, 90

[13] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," in *IEEE Journal on Selected Areas in Communications*, vol. 18, March 2000, pp. 535 –547. 6, 11, 12, 13

[14] A. Kumar, E. Altman, D. Miorandi, and M. Goyal, "New Insights from a Fixed Point Analysis of Single Cell IEEE 802.11 WLANs," in *Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Infocom 2005*, vol. 3, 2005, pp. 1550–1561. 6, 7, 11, 25, 33, 39, 44

[15] G. Kuriakose, S. Harsha, A. Kumar, and V. Sharma, "Analytical Models for Capacity Estimation of IEEE 802.11 WLANs using DCF for Internet Applications," *Wireless Networks*, vol. 15, no. 2, pp. 259–277, February 2009. 6, 11, 46

[16] P. Chatzimisios, A. Boucouvalas, and V. Vitsas, "IEEE 802.11 Packet Delay - A Finite Retry Limit Analysis," *Global Telecommunications Conference, Globecom '03*, pp. 950–954 Vol.2, 2003. 6, 12

[17] M. M. Carvalho and J. J. Garcia-Luna-Aceves, "Delay Analysis of IEEE 802.11 in Single-Hop Networks," in *ICNP '03: Proceedings of the 11th IEEE International Conference on Network Protocols*, 2003, pp. 146–155. 6, 12

[18] P. Raptis, V. Vitsas, K. Paparrizos, P. Chatzimisios, A. C. Boucouvalas, and P. Adamidis, "Packet delay modeling of IEEE 802.11 Wireless LANs," in *International Conference on Cybernetics and Information Technologies, Systems and Applications*, 2005. 6, 12

[19] M. Özdemir and A. B. McDonald, "An M/MMGI/1/K Queuing Model for IEEE 802.11 ad hoc Networks," in *PE-WASUN '04: Proceedings of the 1st ACM International Workshop on Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks*, 2004, pp. 107–111. 6, 12

[20] D. Miorandi, A. A. Kherani, and E. Altman, "A Queueing Model for HTTP Traffic over IEEE 802.11 WLANs," *Computer Networks*, vol. 50, no. 1, pp. 63–79, 2006. 6, 12, 13

[21] H. Zhai, Y. Kwon, and Y. Fang, "Performance Analysis of IEEE 802.11 MAC Protocols in Wireless LANs," *Wireless Communications and Mobile Computing*, vol. 4, no. 8, pp. 917 – 931, 2004. 6, 12

[22] J. Zhu and H. Yin, "Enabling Collocated Coexistence in IEEE 802.16 Networks via Perceived Concurrency," *IEEE Communications Magazine*, vol. 47, no. 6, pp. 108–114, June 2009. 8, 14

[23] X. Yang, X. Yang, J. Zhu, and H.-Y. Liu, "Collocated Radio Coexistence Method," USA Patent US 7 907 572B2, 03 15, 2011, http://www.patentlens.net/patentlens/patent/US_7907572B2/. 8, 14

[24] M. M. Siddique, B.-L. Wenning, C. Gorg, and M. Muehleisen, "Spectrum Sharing between IEEE 802.16 and IEEE 802.11 based Wireless Networks," in *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM)*, June 2010, pp. 1 –6. 8, 14

[25] N. J. Thomas, M. J. Willis, and K. H. Craig, "Analysis of Co-existence between IEEE 802.11 and IEEE 802.16 Systems," in *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, vol. 2, Sept. 2006, pp. 615 –620. 8, 14

[26] J. Kim, S. Park, S. Rhee, Y.-H. Choi, and H. Hwang, "Energy Efficient Coexistence of WiFi and WiMAX Systems Sharing Frequency Band," in *Future Generation Information Technology*, ser. LNCS, vol. 6485, 2010, pp. 164–170. 8, 14

[27] C. F. Chiasserini and R. R. Rao, "Coexistence Mechanisms for Interference Mitigation between IEEE 802.11 WLANs and Bluetooth," in *IEEE Infocom*, vol. 2, 2002, pp. 590 – 598. 8, 15

[28] O. Dabeer, "Improved Capacity and Grade-of-Service in 802.11-Type Cell with Frequency Binning," *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 4176–4184, November 2008. 11, 19

[29] C. Bordenave, D. Mcdonald, and A. Proutire, "Random Multi-access Algorithms - A Mean Field Analysis," INRIA, France, Tech. Rep. 5632, 2005. 11, 40

[30] A. Zanella and F. D. Pellegrini, "Statistical Characterization of the Service Time in Saturated IEEE 802.11 Networks," *IEEE Communication Letters*, vol. 9, no. 3, pp. 225–227, March 2005. 12

[31] P. Raptis, K. Paparrizos, P. Chatzimisios, and A. C. Boucouvalas, "Packet Delay Distribution of the IEEE 802.11 Distributed Coordination Function," in *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM 2005*, 2005, pp. 299–304. 12

[32] S. G. Sitharaman, "Modeling Queues using Poisson Approximation in IEEE 802.11 Adhoc Networks," in *Local and Metropolitan Area Networks, 2005. LANMAN 2005*, 2005, pp. 18–21. 12

[33] A. Abdrabou and W. Zhuang, "Service Time Approximation in IEEE 802.11 Single-Hop Ad Hoc Networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 1, pp. 305–313, January 2008. 12

[34] B. Jang and M. L. Sichitiu, "IEEE 802.11 Saturation Throughput Analysis in the Presence of Hidden Terminals," *IEEE Transactions on Networking*, vol. 20, no. 1, pp. 557–570, April 2012. 12

[35] J. Zhang and X. Ma, "Broadcast performance analysis of IEEE 802.11 networks under fading channels," in *Proceedings of International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 2013, pp. 18–21. 12

[36] J.-H. Yun, "Performance analysis of IEEE 802.11 WLANs with rate adaptation in time-varying fading channels," *Computer Networks*, vol. 57, no. 5, pp. 1153–1166, April 2013. 12

[37] O. Tickoo and B. Sikdar, "A Queueing Model for finite load IEEE 802.11 Random Access MAC," in *IEEE International Conference on Communications 2004*, vol. 1, June 2004, pp. 175–179. 13

[38] Y. Zheng, K. Lu, D. Wu, and Y. Fang, "Performance Analysis of IEEE 802.11 DCF in Binary Symmetric Channels," in *Global Telecommunications Conference, 2005. Globecom '05*, 2005, pp. 3144–3148. 13

[39] O. Tickoo and B. Sikdar, "Queueing Analysis and Delay Mitigation in IEEE 802.11 Random Access MAC based Wireless Networks," in *Infocom 2004*, 2004, pp. 1404–1413 vol.2. 13

[40] S. H. Nguyen, H. L. Vu, and L. L. H. Andrew, "Performance Analysis of IEEE 802.11 WLANs With Saturated and Unsaturated Sources," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 333 – 345, January 2012. 13

[41] G. J. Sutton, R. P. Liu, and I. B. Collings, "Modelling IEEE 802.11 DCF Heterogeneous Networks with Rayleigh Fading and Capture," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3336–3348, August 2013. 13

[42] "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements — Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)," *IEEE Std 802.15.1-2005*, 2005. 14

[43] RoofNet, "MIT RoofNet Project," http://pdos.csail.mit.edu/roofnet/. 19

[44] C. E. Perkins, *Ad Hoc Networking: An Introduction*. Addison-Wesley Longman Publishing Co., Inc., 2001. 19

[45] S. Soundararajan and P. Agrawal, "A Scheduling Algorithm for IEEE 802.16 and IEEE 802.11 Hybrid Networks," in *Broadband Communications, Networks and Systems, 2007. Broadnets 2007*, 2007, pp. 320–322. 19

[46] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," *Computer Networks*, vol. 47, no. 4, pp. 445 – 487, 2005. 19

[47] "NS-2, *The ns-2 network simulator*," http://www.isi.edu/nsnam/ns. 20

[48] "OPNET Modeller, *The OPNET Modeller version 11.5*," http://www.opnet.com. 20

[49] "QualNet Developer, QualNet Analyzer, version 4.1 *Scalable Network Technologies*," http://www.scalable-networks.com. 20, 25, 29, 42, 80

[50] D. H. A., *Order statistics*, 2nd ed. John Wiley, 1981. 27

[51] D. Bertsimas, K. Natarajan, and C.-P. Teo, "Tight Bounds On Expected Order Statistics," *Probability in the Engineering and Informational Sciences*, vol. 20, no. 4, pp. 667–686, 2006. 27

[52] N. Papadatos, "Maximum Variance of Order Statistics," *Annals of the Institute of Statistical Mathematics*, vol. 47, no. 1, pp. 185–193, January 1995. 28

[53] "MATLAB - The Language of Technical Computing, version 7.10.0 (R2010a) *The MathWorks Inc.*" www.mathworks.com/products/matlab/. 29

[54] V. Ramaiyan, A. Kumar, and E. Altman, "Fixed Point Analysis of Single Cell IEEE 802.11e WLANs: Uniqueness and Multistability," *Transactions on Networking*, vol. 16, no. 5, pp. 1080–1093, October 2008. 33

[55] L. Kleinrock, *Queueing Systems - Theory, Volume 1*. Wiley-Interscience, 1975. 41

[56] W. Rudin, *Principles of Mathematical Analysis*. McGraw-Hill Publishing Co., September 1976. 41

[57] Wireshark, "Network Protocol Analyzer," http://www.wireshark.org/. 56, 99

[58] "TP-Link TL-WN350GD PCI card, Atheros based IEEE 802.11 PCI Wireless Card," http://www.tp-link.com/en/products/details/?model=TL-WN350GD. 56

[59] "Linksys WRT54GL, A Linux Capable IEEE 802.11b/g Flexible Wireless Router," http://support.linksys.com/en-us/support/routers/WRT54GL. 57

[60] "Linux Distribution for Embedded Devices," http://www.openwrt.org. 57

[61] "Information Networks Laboratory, Department of Electrical Engineering, Indian Institute of Technology Bombay, Powai, Mumbai, India." [Online]. Available: http://www.ee.iitb.ac.in/~infonet/ 58

[62] Madwifi, "Madwifi Project," http://www.madwifi-project.org. 60, 99

[63] "The /proc File System," http://www.kernel.org/doc/Documentation/filesystems/proc.txt. 62

[64] "*iperf*: Internet Protocol Traffic Generator," http://iperf.sourceforge.net/. 63, 100

[65] "*udpmon*: A Software Tool for Testing Hardware and Network Behaviour using UDP," http://www.hep.man.ac.uk/u/rich/net/. 63

[66] brute, "Brawny and RobUst Traffic Engine," https://code.google.com/p/brute/. 63

[67] J. Kulbatzki, *Das Programmsystem PRIORI -Erweiterung und Validierung mit Simulationen.Diplomarbeit*. University of Erlangen, 1989. 78

[68] R. Aiello and S. Shetty, "Testing Raises Concerns over 802.11-based High-speed Bluetooth," *EE Times*, March 2008, http://eetimes.com/design/automotive-design/4012958. 87, 90

[69] S. Zhan, A. Waltho, X. Guo, C. Chen, and A. Bettner, "Performance Analysis and Design Considerations for Multi-Radio Platforms," *Intel Developer Forum Report*, 2006. 87, 90

[70] "Recommendations On Allocation and Pricing for 2.3-2.4 GHz, 2.5-2.69 GHz & 3.3-3.6 GHz bands, Telecom Regulatory Authority of India (TRAI)." [Online]. Available: http://www.trai.gov.in/content/RecommendationDescription.aspx?RECOMEND_ID=311&qid=21 88

[71] E. G. Villegas, E. Lopez-Aguilera, R. Vidal, and J. Paradells, "Effect of Adjacent-Channel Interference in IEEE 802.11 WLANs," in *Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, August 2007, pp. 118 –125. 88

[72] "InSSIDer, WiFi Network Scanner by *MetaGeek*." [Online]. Available: http://www.metageek.net/products/inssider 89

[73] "IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Broadband Wireless Access Systems," *IEEE Std 802.16m*, 2011. 92

[74] "Qualcomm Atheros," www.atheros.com. 99

[75] "Realtek RTL8187 USB, IEEE 802.11b/g wireless adapter with a USB interface," http://www.realtek.com/downloads/searchView.aspx?keyword=rtl8187. 99

[76] 802.11 Ninja, "Loss Of Radio CONnectivity (LORCON2)," http://802.11ninja.net/. 99

[77] P. Rathod, O. Dabeer, A. Karandikar, and A. Sahoo, "Characterizing the Exit Process of a Non-Saturated IEEE 802.11 Wireless Network," in *Proc. of ACM Mobile Ad Hoc Networking and Computing (MobiHoc '09)*, 2009, pp. 249–258. 102

[78] W. J. Reed and M. Jorgensen, "The Double Pareto-Lognormal Distribution - A New Parametric Model for Size Distributions," 2003. 109

[79] L. A. Adamic and B. A. Huberman, "Zipf's law and the Internet," *Glottometrics*, vol. 3, pp. 143 – 150, 2002. 109

[80] M. Gast, *802.11 Wireless Networks: The Definitive Guide*. OŔeilly Media, 2005. 113

[81] R. Rom and M. Sidi, *Multiple Access Protocols: Performance And Analysis*. Springer, 1990. 113

[82] A. O. Allen, *Probability, Statistics and Queueing Theory - with Computer Science Applications (2nd edition)*. Academic Press, 1990. 115

List of Publications

[1] P. Rathod, O. Dabeer, A. Karandikar, and A. Sahoo, "Characterizing the Exit Process of a Non-Saturated IEEE 802.11 Wireless Network," in *Proc. of ACM Mobile Ad Hoc Networking and Computing (MobiHoc '09)*, 2009, pp. 249–258.

[2] ——, "Towards the Performance Analysis of IEEE 802.16 Backbone Mesh Networks," in *Proc. of S3 Workshop, ACM Mobile Ad Hoc Networking and Computing (MobiHoc '09)*, 2009, pp. 9–12.

[3] P. Rathod, A. Karandikar, and A. Sahoo, "Facilitating Non-Collocated Coexistence for WiFi and 4G Wireless Networks," in *Proc. of IEEE International Conference on Local Computer Networks (LCN '12)*, 2012, pp. 1–9, Best Paper Candidate.